

Thomas M. Jacobius  
Director, IPRO Operations & External Relations  
The Interprofessional Projects Program  
Idea Shop at Technology Business Center  
3440 South Dearborn Street, Suite 050  
Chicago, Illinois 60616  
P: 312-567-3986  
F: 312-567-3609  
[jacobius@iit.edu](mailto:jacobius@iit.edu)  
<http://ipro.iit.edu>

November 14, 2014

Marlene H. Dortch, Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

Re: ET Docket No. 14-143 Mobile Device Theft Prevention and Changes in the Mobile Device Theft Prevention Working Group

On behalf of 24 multidisciplinary student teams completing the Interprofessional Course at Illinois Institute of Technology (IIT) during the fall 2014 semester, we are pleased to submit their concepts to address mobile device theft protection. The following pages consist of:

- Overview of the IIT Interprofessional Projects (IPRO) Program
- Summary of the “FCC Mobile Device Theft Protection Challenge” process undertaken by IIT student teams
- Concepts developed by IPRO teams and hereby submitted as public comments.

### **I. Overview of the IIT Interprofessional Projects Program**

The IPRO Program Mission Statement is to “Provide IIT students with an exemplary experience in making contributions as part of a high performance multidisciplinary team by applying professional methods in a rigorous fashion to develop viable solutions that create value.” The overarching aim is to foster in our future leaders a spirit of collaborative innovation that will sustain them in their chosen professions and careers.

The highly experiential, open-ended problem solving Interprofessional Project course is characterized as follows:

- **Purpose:** fulfill a distinctive general education requirement whereby all undergraduates complete two three-credit-hour multidisciplinary IPRO team project courses.
- **Topics:** reflect the diversity of the workplace (corporations, new ventures, non-profit organizations, government agencies and academic research)
- **Teams:** multidisciplinary collaboration that demands teamwork, communication, logically-correct reasoning, project management and awareness of ethical issues.
- **Emphasis:** user-centered design thinking methods from the Institute of Design at IIT that span problem framing, fieldwork and observation that reveals insights, brainstorming, synthesis, iterative prototyping and creation of an opportunity assessment with value proposition.

*Interprofessional* education refers to the teaching and learning of students from different professions together during all or part of their professional training in order to promote collaborative working in their professional practice. (Source: Wikipedia)

There are three prominent IPRO Course Learning Platforms:

- Interprofessional by design workshop
  - Faculty team taught
  - Foundation in user-centered design methods
  - Incubating new concepts
- Traditional single topic IPRO team
  - Personalized faculty coaching
  - In-depth problem solving with a sponsor or community partner
- Themed clusters
  - IPRO topics aggregated under broad problem areas, including:
    - STEM Education
    - Community Engagement
    - Urban Agriculture
    - Made in USA: Re-Making in America
    - Student New Venture Accelerator
  - Teams develop understanding of broad context and share and collaborate across teams for mutual benefit

The scale of the IPRO Program is reflected in its demographics each semester:

- 600 to 800 students
  - Predominantly juniors and seniors
  - Representing architecture, business, engineering, the sciences, humanities and social sciences, psychology, and applied technology
- 70 to 80 multidisciplinary teams
  - Ranging in size from 5 to 20 students
  - Representing at least three different IIT colleges
- 30+ instructors representing all IIT fields of study
  - Regular tenured and tenure-track faculty as part of teaching load
  - Part-time faculty with industry experience
- 20+ sponsors and community partners.

## **II. The IPRO Team Mobile Device Theft Challenge Process**

The IPRO Team Mobile Device Theft Challenge was offered to the IPRO course participants by Dennis Roberson, Vice Provost for Research & Research Professor, and Chairman of the FCC Technological Advisory Council. Dr. Roberson visited the two IPRO workshop course sections and provided context by framing the nature and extent of the mobile device theft problem for the IPRO teams in attendance. His presentation underscored the complexity, magnitude, pervasiveness and growth of the problem experienced by consumers and affecting a range of sectors participating in the mobile device and services industry.

Following this overview presentation and Q&A session, IIT's 24 IPRO teams of 5 or 6 students from multiple disciplines devoted one month, spanning September and October 2014, to rapidly undertaking the following user-centered design methodology:

- Conducting research (secondary and primary)
- Characterizing user/stakeholder needs (consumers, carriers, manufacturers, government agencies, offenders)
- Developing specifications
- Creating a taxonomy
- Brainstorming concepts

- Documenting work

The participants in the two IPRO workshop sections are comprised of 129 students organized in 24 multidisciplinary teams. The disciplines represented from all IIT undergraduate colleges consist of the following: aerospace engineering, applied mathematics, architecture, architectural engineering, biology, biomedical engineering, business administration, computer information systems, chemical engineering, chemistry, civil engineering, communication, computer engineering, computer science, electrical engineering, information technology management, materials science and engineering, mechanical engineering, political science, professional and technical communication, and psychology.

### **III. IIT IPRO Team Concepts Submitted as Public Comment**

We are pleased to submit the concepts developed by 24 IPRO teams on their behalf and under the guidance of faculty teams led by Jeremy Alexis, Senior Lecturer, Institute of Design and Director, IPRO Program. The teams are listed below, followed by their concept presentations. The concepts encompass three main areas of concern associated with the mobile device experience, namely consumer awareness, theft deterrence, and theft tracking and/or neutralization of mobile device function and content:

Tuesday Evening Teams Enrolled in IPRO 397-300 Interprofessional by Design Workshop

- IPRO Team T1A: STEPS
- IPRO Team T1B: Safe Band
- IPRO Team T2A: Ghost Phone
- IPRO Team T2B: The Leash
- IPRO Team T3A: NxtGen Theft Solution
- IPRO Team T3B: The Tether
- IPRO Team T4A: SleekID
- IPRO Team T4B: PSA
- IPRO Team T5A: Cryptone
- IPRO Team T5B: Prism
- IPRO Team T6A: Chain Reaction
- IPRO Team T6B: Virtual Leash

Wednesday Afternoon Teams Enrolled in IPRO 397-400 Interprofessional by Design Workshop

- IPRO Team W1A: The Deadbolt
- IPRO Team W1B: The Excommunicator
- IPRO Team W2A: Bi-Optic Antitheft System
- IPRO Team W2B: LifeBoard+LifeRing
- IPRO Team W3A: Phone Prevention
- IPRO Team W3B: G-Lock
- IPRO Team W4A: Strap+Batt+Track+Store
- IPRO Team W4B: Phone Security
- IPRO Team W5A: Alert Systems
- IPRO Team W5B: SafeMode
- IPRO Team W6A: The PIDDS
- IPRO Team W6B: Tracking+Proximity

Respectfully submitted,



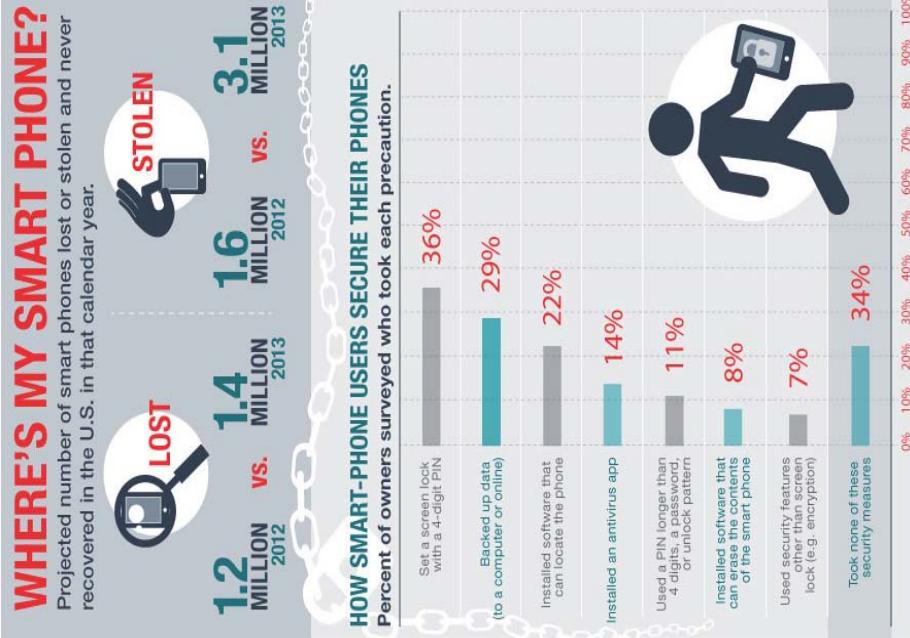
# S.T.E.P.S

(Solutions That Enable Phone Security)

Presented by: Donna Calabria, Ryan Eggert, Chang Liu, Mikel Polena, Xiaojing Wang  
IIT IPRO Team T1A

# CONCEPT

According to statistics,  
**64%** of smart-phone users  
do not set a pin for their  
phones. As a result our  
group focused on  
**INCREASING PHONE  
SECURITY.**



© 2014 Consumer Reports. All rights reserved

**ConsumerReports**

# MANDATORY PINs

When someone purchases a smart-phone he is obliged to set-up a pin. Even the simplest pin can prevent ease of access and keep all your information secured.

**Authenticate**

Password / PIN:

**Authenticate**      **Cancel**

# AIRPLANE MODE PIN

Aside from that a mandatory airplane mode pin is also required. By having this pin, the thief would not be able to set your phone to airplane mode. So all the connections will not be disabled.

# CREDIT CARD PHONE

The user's information is given to the phone provider to determine "regular/normal" phone usage patterns. By doing this the owner gets notified of unusual activity and requires user to verify identity. You may not always be aware that your device is missing so this provides a preemptive notification for original owner of device via email.

# SECONDARY SECURITY DEVICE

A watch, bracelet, pin, button or clip that is easy to hide. Automatic proximity distress call that lets you know if your phone is out-of-range. If someone steals your phone, you can manually reset it. Securing all your information stored in your phone. The result provides fast and reliable way to erase data. It is portable, easy to hide and convenient. Lastly, this security device provides way for owners of stolen device to act faster.

# RISK

- Giving your information through phone providers can result in potential loss of privacy which can get hold of your information getting hacked.
- If the user has irregular pattern of usage, the system might generate too many alerts that can be a nuisance

# MITIGATIONS

- Providing a way to disable the feature by double authentication
- Setting up a law that would prevent phone providers from sharing your personal information to third parties

# IMPLEMENTATION GUIDANCE

- Requiring manufacturers to set-up the device operating system to mandate user pins
- Implementing a Federal Law that would protect User's personal information from being shared

# Jean's Case:

Jean just got out of the library at night after studying for hours. As she was walking she decided to contact her friend. Little did she know that there was someone watching her, thinking of stealing her phone. The thief waited for the opportune moment, grabbed her phone and started running away. However, the thief did not know that Jean's phone was secure. He tried switching it into airplane mode but was not able due to password protection that she had on the device. Needless to say the thief was unable to access her phone. However, Jean did not feel comfortable with the idea that someone else had her phone. In order to protect her personal information she decided to erase her data with the help of her secondary device. When she went home she notified her cell phone provider that her phone got stolen. Despite her phone being stolen Jean took several STEPS to protect her identity and render her phone unusable.

# Safe Band



IIT IPRO Team T1B

Mickaele Perez

Hui Mink Khor

Timothy Ragin

Liliana Gonzales

Nallely Silva



All of us have encountered different cell phone theft situations that make us vulnerable to robbers. Safe band is a great way to have control over your phone anytime, everywhere. Safe band solves different problems in which today's thefts are targeting cell phones. **Identify Theft** when phone is being stolen, **Data Security** as soon as Safe Band is activated, Safe Band will activate different features in which the phone cannot be accessible.



## Alternatives

- Concepts that were considered:
  - Solder everything in phone so that the thief can't access components
  - Customize every component in the phone so nothing is the same
  - Phone uploads a virus to computer if it is accessed through an unknown device
  - Phones can only be sold and traded to phone company

## Specifications/Criteria

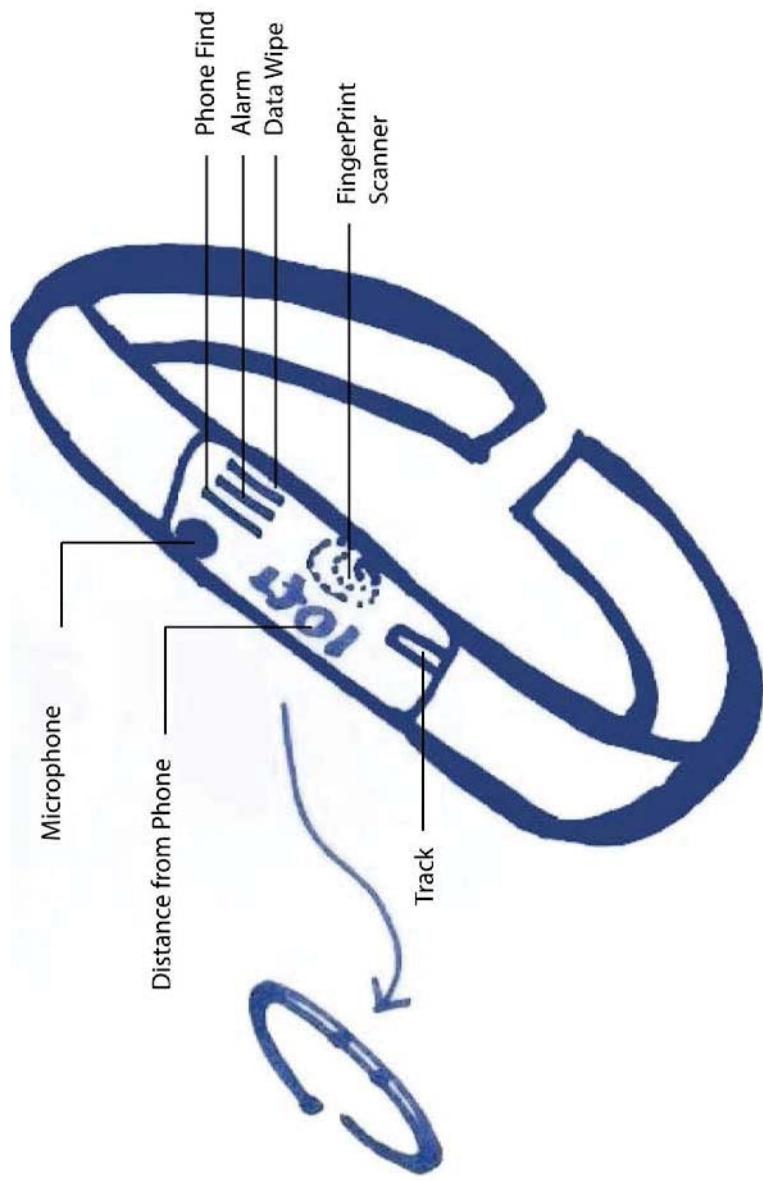
- The concept needs to meet the following:
  - Protects user's data
  - Prevent phone from being stolen
  - Make retrieving stolen phone easier
  - Make it appealing to the user
  - Easily accessible to the user
  - Efficient and plausible



## How It Works?

- The Safe Band increases the security of cell phones by implementing distance based and voice activated features that deter would be criminals from attempting to steal the device.
- When the phone is stolen, the wearer of the Safe Band can either yell after their phone, or press a button on the Safe Band that will cause the phone to emit a loud, repetitive sound that cannot be deactivated by the thief. This can also be configured to activate via distance from the wristband.
- Data is remotely wiped from the phone when this process is implemented, and can be restored via backups if the phone is reunited with it's owner.
- Bluetooth pairs Safe Band with phone and allows is the means of tracking the distance from the phone and sending commands to it.
- Fingerprint scanner is used to ensure that security measures can only be disabled by device owner
- Microphone senses user's voice and can trigger security features when the user says certain words or phrases.
- Basic file encryption used to increase data security on device and prevent unauthorized access to phone contents.
- Device will infect unauthorized computers with viruses if password failure occurs 5 times.
- Phone will come with embedded tracking device that operates independently of the phone itself. If the device is reported stolen, it's location will be tracked.

## Safe Band Design





## Scenario of Use

- This device works primarily in the case where someone is attempting to steal a smartphone from the individual in possession of the Safe Band.
- The device allows its owner to make verbal commands that are then given to the phone to activate security features.



## Stakeholders' Value Propositions

### **Consumers**

-Our product will increase data security and decrease theft. Users will save money by eliminating the cost of replacing stolen phones. Safe Band is a trendy, innovative, proactive solution to phone theft.

### **Carriers**

-Frustrated carriers will decrease the amount of calls they will get about theft and will decrease the amount of phones they have to replace through insurance claims. Carriers that promote Safe Band will gain consumer appreciation by showing concern for the safety of user information and phone theft.

### **Government**

- Cell phone theft has become a huge safety concern for the government. Phone theft creates violence, identity theft, and negatively impacts the economy. Safe Band's features combat these negative factors.

### **Device Makers**

-Companies that invest in the production of Safe Band will increase safety for phone users (75% of the world- RFERL) and have a potential market of 5.34 billion consumers.



### **Core Capabilities**

- Differentiation: No other product out there.
- Experience: Many team members have had their phone stolen.
- Generation: Team has lived through mobile development and outburst.

### **Business Model**

**Cost**  
-Estimated between \$50-\$100

### **Management**

- Leadership
- Organization
- Communication

### **Distribution**

- Mobile carriers
- Electronics
- Industry
- Online
- Retailers



## Mitigations

### User

- Self-safety is more concerned
- More expense

### Stakeholder

- Big project for every features to be included and be available
- Big investment before making any sales



## Implementation Guidance

Stakeholder's part in research and development (hardware and software) and as well as the installation.

Customer's part in giving out necessary information and data to the stakeholder.

Patience from every side

IIT IPRO Team TA2

Prof. Stephen Hammond

Mobile Device Theft Prevention Challenge  
GhostPhone- A Cloud-Based Solution

Alden Rose

Aldo Maldonado

Guillermo Colin

Majed Abdulsamad

Maxine Mawussi

Sukrins Shrestha

**Why Our Idea?**  
**User Specifications**  
**Selection Process**  
**Detailed Description**  
**Scenario of Use**  
**Stakeholder Benefits**  
**Business Model**  
**Risks / Mitigation**  
**Implementation**

# Why our idea ?

Our Idea presents a solution that reduces phone theft significantly and will eventually lead to ending this phenomenon.

We are calling our idea; Ghost Phone. It aims to:

- **Devalue the device- Hardware and Software**  
(prevent selling the whole or parts of the device, and prevent identity theft )
- **Protect personal information on the device.**
- **Raise awareness among users.**

# User Specifications

Needs	Metrics	Target specifications
Campaign to raise awareness	Information freely accessible to consumers	1 notification a month (in a form of an ad. or a text)
Ease of use	Number of steps to operate	Less than 6 steps
Devalue the device (Hardware)	value of the device as a physical object	decrease price of device, increase value of plan, storage
Devalue the device (Info.)	Number of personal accounts	Less than 4 accounts
Cost efficiency	Price of installation of software	Less than 10% of price device

# Selection process

Our final selection was favored for:

1. Ease of operation
2. Absolute safety for user

It is a web based operating system that shall be the core for the future of web security. As a matter of fact it, this type of software has shifted from long to short term goals for numerous software developing firms in the US. It is a matter of months before these softwares become the default in the world of smart devices.

Other alternatives of ours included control of the battery that would enable the user to manipulate the heat or the chemicals of the battery in ways that could damage the phone based on speed of movement, attempts to force open or provider signals. However, it's impossible to fully protect user in case of false alarms. Therefore we decided to give up on this solution and invest in a safer more reliable solution.

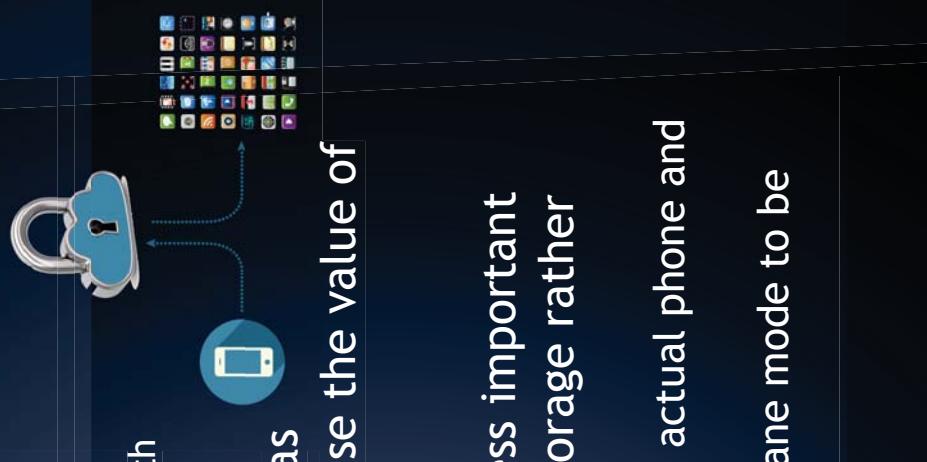
# Detailed Description

A new operating system would be developed, very similar to currently existing Chrome OS by Google. Like Chrome OS, this software would run the phones with an emphasis on web apps as opposed to native apps.

The main idea here is to have the phone to be as web based as possible to keep data off the physical device, this will decrease the value of the hardware and increase the importance of the software.

Without proper authentication it would be impossible to access important information on the phone due to it being saved using cloud storage rather than physically on the phone.

The software on the phone would be the minimal required to run the actual phone and it would retrieve appdata entirely through internet access.  
With previous authorization by user, the phone can be put in a air-plane mode to be used off the internet for a certain amount of time (e.g. on a plane)



# Scenario of Use

A user with a “Ghost” phone just needs to set up a Pin Code like any other smartphone to ensure that their phone is locked. With permanent Internet connection, the phone is a platform for any app the user needs to use. If out of sight of user, the phone can not be shut off or switched to air-plane mode without typing the code. A code that can’t be broken through typical Pin Code breaking softwares due to a firewall in the cloud that identifies any breaking attempts. However, the phone always operates in cases of emergency to call 911.

The phone can not be used by different users because it is locked to one carrier, a carrier that has the phone software data and access codes. Therefor, the carriers are the only ones to sell or buy the used phones before setting them up for new users.

Devaluing the phone had to mean a new design strategy for the hardware, a solid one block that contains all the phone components put together in a sealed cover. A sample of this design is already in use by Apple for their product (Mac BookPro).

We at IIT were able to print a 3D cover for the phone. Providers can have this 3D printed one piece-shell wrap around the device components without screws making it impossible to break in the phone without damaging it beyond repair. A case that could only be opened by the manufacturer.

# Stakeholder Benefits

## Providers

### New design

new opportunities  
wider design options  
lighter and smaller shapes  
cheaper product

## Carriers

### New plans

unlimited data  
cloud storage options

## Users

### Higher Phone security

More reliable service

Unlimited access to

### the internet

Smaller, lighter devices

## Expand services

Wider coverage  
personal data control  
Insurance plans

## New Market

bigger need  
various marketing options

# Business Model

Providers	Carriers	Users
Hardware design	Provide data plans	Pay for devices
Develop software	Store clients data	Pay for cloud storage
Contribute to the awareness campaign	Lead the awareness raising campaign	Benefit from new phone secure design
Device manufacturing		

## Risks/ Mitigation

- Providers not willing to invest in higher security level in mobile devices.
- Carriers not offering convenient data plans to users.
- Emphasising the importance of web security.

# Implementation

The “Ghost” phone is a higher level of security that can be provided for users in the US for now and soon for the rest of the world. This phone does not replace the existing huge smart device market, but presents an alternative for those not satisfied with the level of security they have on their phones.

This new design, once providers start manufacturing and advertising it, shall encourage software developers and entrepreneurs to invest their time and money in this new generation of open source systems and bring new revolutionary ideas to the table.

From that point on, users will start having various options and eventually will be able to customize their own security system as they feel appropriate.

Thank you

# The Leash

IIT IPRO Team T2B: Joel Greggio, Huy Bui, Clare Dorin, Brahadon Ramirez, Joe Boesso, Mazen Ataya

# Why reinvent the wheel?

Utilization industry standards for information protection

- Full disc encryption
- Crypto-Chip

A secondary device that directly connects the user to their phone (similar to a “Smart key” for your car)

- Without this device, access to the data stored on the phone is blocked

# Why The Leash is Necessary

- Secure personal information
- Directly connect the user with their phone
- Alert user to the theft
- Instant solution to theft
- Provide a way to connect to provider

# Alternatives considered

The phone itself will always be expensive

- cannot prevent thieves from stripping it for parts
- replacing phone while annoying, still possible

Recovery of phone

- chasing thief is dangerous and unwise
- complete destruction of phone is an extreme response if only misplaced

Therefore...

**The most valuable feature of a smartphone  
is the stored personal data**

## Full Disc Encryption w/ Crypto-chip

Currently used by fortune 500 companies to protect sensitive information on employee laptops.

- Full disc encryption: the conversion of information into unreadable code that cannot be accessed or deciphered by unauthorized individuals
- While currently an option, the extra processing needed slows functionality

Crypto-chip: a secure cryptoprocessor embedded in the motherboard that can be used to authenticate the device.

- ‘mini processor’ devoted to decryption (i.e. functionality remains fast)
- Ties the hard drive to a particular device.
- If it is removed and placed in another, the decryption process will fail.

# The Leash

A secondary device connected to the smartphone.

- phone's antenna and a radio pulse generator in The Leash housing

If the device is outside a specified range, the phone automatically performs an action.

- Range and action can be specified by the user

A password is then needed to restart the operating system.

- rotating and randomized

The Leash can also come in a variety of styles with different features.

- A ring, keychain, ‘business card’ for wallet
- Panic button, button connected to provider (similar to “OnStar”)

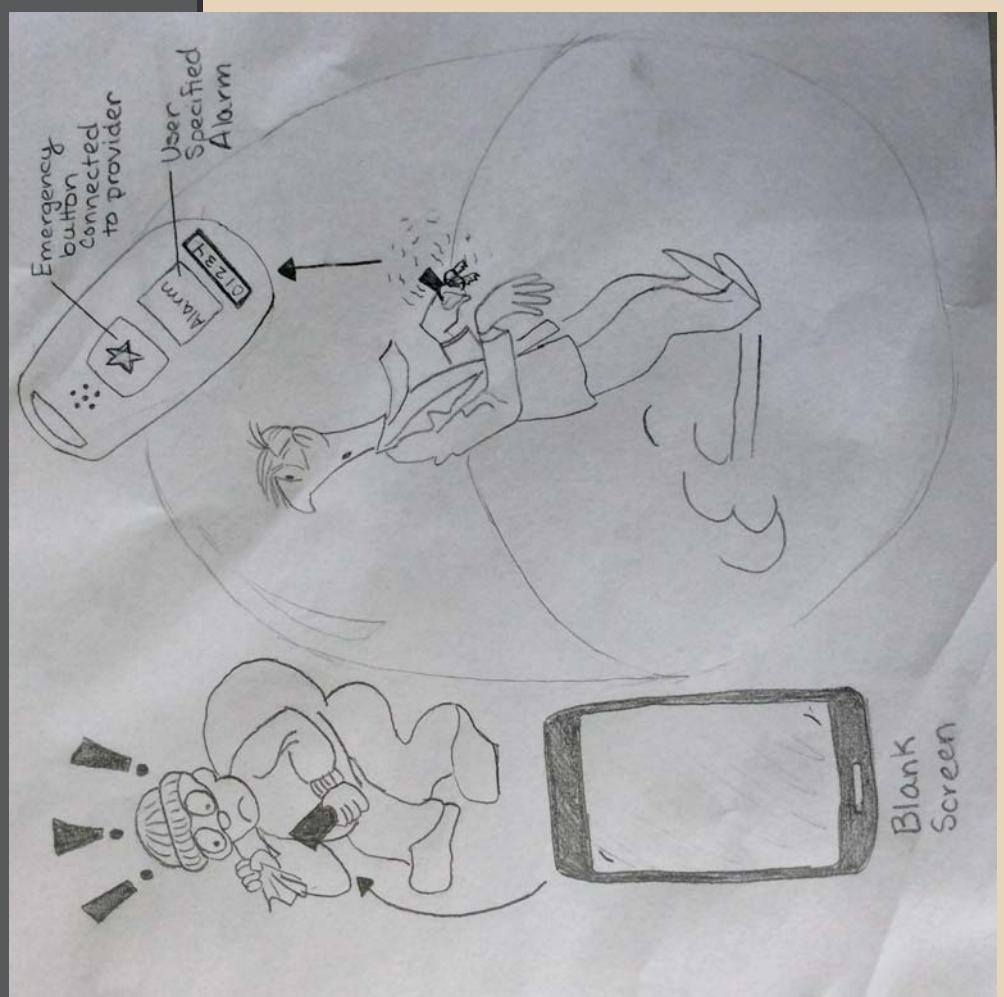
# Scenario

The Leash will alert the business man when his phone is outside the specified range.

The thief will be unable to access the encrypted data because the touchscreen will be inactive.

If the thief runs away, push the emergency button to contact your provider.

If recovered, simply enter the randomized password to access the operating system.



# Stakeholders

The values for stakeholders can be viewed in two different aspects:

	<b>Economic aspect</b>	<b>Social aspect</b>
<b>Consumers</b>	- Save money on device replacement	- Secure personal data - Complete control over the access to the device
<b>Carriers</b>	- Increase annual profit by providing the service	- Save money on labor - Gain reputation for service's quality
<b>Government</b>	- Increase revenue from tax for further development in other fields	- Save money on labor for extra protection - Gain access to theft identity for further investigation of crime-committed organization
<b>Device maker</b>	- Gain profit through sales - Generate more businesses by partnering with carriers (network providers).	- Gain reputation for strengthening the consumer's security of personal data - Contribute to the reduction of phone theft cases

# Business Model

<b>Key Partners</b> Who are our Key Partners	<b>8</b> <b>Value Propositions</b> What value do we deliver to the customer?	<b>7</b> <b>Key Activities</b> What Key Activities do our Value Propositions require	<b>2</b> <b>Customer Relationships</b> What type of relationships do our Customer Segments expect?	<b>4</b> <b>Customers Segments</b> Who are we creating value for?
Companies that provide Encryption for devices	Making sure that our product protect our consumers from theft	Safety for themselves and their surrounding environment	Trust	Law enforcement
Cell Phone Carriers	Creating a second device and encryption	Identity Theft Protection	Secure	Cell Phone Carriers
Law Enforcement	2	3	Informative	Everyone who has a smart phone.
The Government	6	4	Connect	
	Key Resources What Key Resources do our Value Propositions require	5	Channels How do we reach our Customer Segments?	
	research on why people steal phones	3	government getting involved about this epidemic	
	What the consumers fear about theft	4	Using the Cell Phone carriers to explain out product	3
	4 Research from law	3	4	3
<b>Cost Structure</b> What are the important costs inherent in our business model?	<b>9</b> <b>Revenue Streams</b> What value are our customers willing to pay for?			
Marketing Costs	Preventing identity theft from cell phone theft			
Building the second device attached to the phone				
				1
				3

## Risks

What if the user loses The Leash?

What if The Leash was stolen also?

Similar to being locked out of your car...

# Implementation

## Encryption

- setting already an option on current models but further research about its effects on processing speed is needed

## The Leash

- Optional for the user
- Utilize a variety of features to match the lifestyle of the user
- Compatible with many different types of smartphones

# Next Generation Theft Solution

IIIT IPRO Team T3A

Ammar Barkat

Kevin Kleczka

John Ramirez

Shiyi Shen

# Standardized Kill Switch

- Software included that erases all data
- Activated over network or set number of incorrect password guesses
  - Who's responsible?
    - OS Manufacturer
      - Integrated into software, implement through account (ie. Google)
    - Default password
      - Incorrect password wipes phone
    - Alternatives
      - Provider install
- Protects privacy
  - Protects data
  - Loss mitigation
  - B2B

# Screen Lock

- When phone is first activated user is required to choose security lock.



ILLINOIS INSTITUTE  
OF TECHNOLOGY

## *The Tether*

IIT IPRO Team T3B

Abraham  
Babatunde  
Hui  
Jenny  
Parnell Prosperis

# Table of Contents

- Introduction
- Approach
- Summarize & Discussion
- Risks & Limitations

# Introduction

The goal of this project defined by the FCC:

- Explored ways that members of the mobile device community (providers, device manufacturers, OS providers, application developers) can improve collaboration with the law enforcement community in a collective effort to thwart mobile device theft
- Addressed ways in which more timely and accurate data about mobile device theft can be made available for both law enforcement entities and others, such as secondary market resellers
- Discussed technology solutions that can limit the theft of mobile devices and curb effects on consumers and businesses

<http://www.fcc.gov/events/fcc-announces-workshop-focus-prevention-mobile-device-theft>

# Approach

- Phone theft is an epidemic in the society & our challenge is to solve this problem.
- Personal Data and hardware are the most important parts of a smart device
- Thus people need security and prevention on these devices are on the rise.

Ways to Accomplish the goal:

- Camera technology
  - The camera will automatically take a photo
- Fingerprint/Eye
  - The touch screen on the phone will be able to scan the fingerprint of the person using it. If the fingerprint does not match any of the registered users; it will raise a red flag.
- Smart Watch
  - The smart watch will be an accessory to the phone

# Solution & Discussion

Smart Watch/Remote Device

If smart device out of range

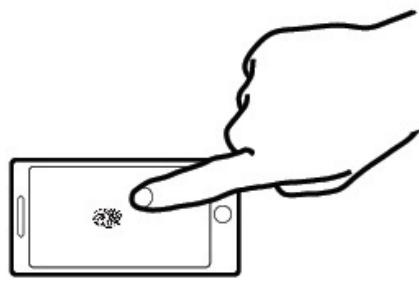
connected to  
smart device



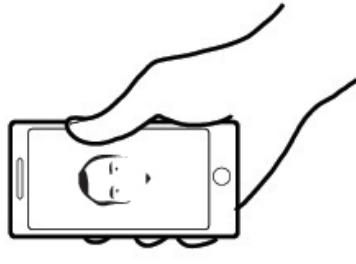
out of range



fingerprint access



automatic takes photo  
of criminal



# Solution & Discussion cont.

## Stakeholders

Economic	Social
<ul style="list-style-type: none"><li>• Carriers<ul style="list-style-type: none"><li>- Increase revenue of service</li></ul></li><li>• Consumer<ul style="list-style-type: none"><li>-Not having to buy a new device</li><li>-Spend money on smart watch and on new features</li></ul></li><li>• Device Makers<ul style="list-style-type: none"><li>-Spending &amp; Earning revenue through this service</li><li>-More business partnering w/ other companies/carriers</li></ul></li><li>• Government<ul style="list-style-type: none"><li>-Tax revenue</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Carriers<ul style="list-style-type: none"><li>- Increase reputation of service protection</li></ul></li><li>• Consumer<ul style="list-style-type: none"><li>-Secure personal data and access to device</li></ul></li><li>• Device Makers<ul style="list-style-type: none"><li>-Reduction in theft</li><li>-Increase reputation</li><li>-Less manufacture of phones</li><li>-Focus more on other important features of devices</li></ul></li><li>• Government<ul style="list-style-type: none"><li>-Increase in time to focus on more bigger crime groups stealing smart devices</li></ul></li></ul>

# Risks & Limitations

- Consumers must buy new features and devices for this to work
- Security measures such as taking photo of criminal, might just wear a mask
- Range of detection
- Fingerprint can be forged
- Criminal can steal the watch and then be able to access the smart device

# SleekID

**Sleek Design with Identification Protection**

Daniel Cuevas  
Naijia Dong  
Juliana Germano  
Mayra Maldonado  
Conner Wiebell  
**IIT IPRO T4A**

# User Needs

- Additional Security
  - Protecting Personal Information
- Unibody device
  - Prevents removal of battery
- Alert system
  - Decreases opportunistic theft

# Alternatives and Criteria

- Non-intrusive
- Convenient for user
- Simple
- User friendly
- Practical design
- Accessible features
- Existing Technology

# Concept Description

- Required password to enable Airplane Mode
- Unibody phone design
- Password protected shutdown feature
- Accessory location device:
  - Alert system when too far from the device
  - Alerts the police if not found in set amount of time
  - Current [kickstarter](#) available, making it a feasible solution

# Usage Scenarios

- The first thing a thief does when stealing a phone is disabling GPS location services by turning it off or enabling Airplane mode. Personal identifiers (passwords) for shutting off and enabling airplane mode will allow owner to have more time to locate the device
- Unibody design prevents thief from simply removing the battery to take the phone off the grid
- Accessory location devices can lock your phone when you're too far from it. Can also alert police about your stolen phone and store the last location of it. Alternative use is a panic button to find your phone if you misplaced it

# Stakeholder Values

- Consumers: Protection of personal information, phone theft prevention
- Carriers: Less insurance claims, consumer attraction for safer phones
- Government: Decrease in illegal phone distribution, Decreased cash flow of organized criminal organizations. Brings insight to the amount of devices stolen and redistributed through criminal organizations
- Device Manufacturers: Higher sales from secure and attractive devices

# Business Model

- Phone manufacturing companies develop only unibody design cellphones.
- Software developers include required personal identifier to enable airplane mode and shut down device using existing technology. Choices between passwords, facial recognition, fingerprint scanner, etc.
- Cell phone providers explain to consumers the importance of using these features in order to increase chances of recovery if theft occurs

# Risks

- Software gets hacked by criminal organizations
- Misuse of safety features, calling the police by accident
- Third party vendors adding back-end code
- Breach of privacy?
- Faulty programs

# Implementation Guidance

- Progression to unibody design from all, if not most, manufacturing companies will allow current phones to fade out over time
- Current buy-back promotions from carriers will allow consumers to trade in their phones and purchase a unibody designed phone for the SleekID features
- Users will be required to have a personal identifier for enabling airplane mode and shutting off device before leaving the store with the new phone

# PSA

## “Phone Security Accessory”

IIT IPRO Team T4B:

Ben Grimmer, Longchen Zhang, Allan Ma, Joshua Quah, Shou Sing, Kierra Herron, Eldridge Lee

## User Needs/ Specifications

Users require a device that prevents phone theft that is convenient and simple.

A system that would enable users to be more aware of their smartphones, thus preventing opportunity theft.

# The PSA System

A PSA is an alarm system that activates when your phone is more than a fixed distance away.

Consumers could choose to buy a PSA.

System consists of:

- A chip on the user (in a bracelet, necklace, shoe, etc.)
- A software application on the user's phone

## The PSA System Details

When the system activates, it could report the incident to centralized database.

The alarm could only be disabled by entering user credentials (password, fingerprint, etc).

## **Benefits of PSAs**

- Effective against opportunity crimes.
- More witnesses when thefts occur.
- Possibility of an alarm is a Crime Deterrent.

## **Benefits of PSAs (cont)**

Device has many varieties and is concealable.

Hearing this alarm will help increase public awareness of phone theft.

- Through the Availability Heuristic<sup>[1]</sup>

[1] [http://www.investopedia.com/university/behavioral\\_finance/](http://www.investopedia.com/university/behavioral_finance/) Phung, Albert. "Behavioral Finance: Key Concept- Overreaction and Availability Bias". Investopedia. February 25, 2009. p.10. December 1, 2013.

## Risk / Mitigation

Risk of encountering physical assault for possession of the PSA in addition to the smart phones.

Solution: PSA hardware comes in different forms (bracelet, pendant etc), which lengthens the time for thieves to obtain PSA by force.

## Possible Extension to Industry

Use of PSA could be encouraged through  
phone insurance providers

- Offering a discount for using it
- Providing hardware for free to consumers

## Possible Extension to Functionality

**Phone could delete sensitive data and disable hardware (“brick” the phone) when stolen.**

- Activated by action on consumer’s PSA device.
- Activated automatically after alarm times out.

## Conclusion

Use of “Phone Security Accessory” could make a major impact on frequency of phone theft.

Progressing this project will next require engagement from hardware producers.

# Cryptone™

## Phone Data Theft Prevention

IIT — IPRO 397 — Group 5A

Rytis Bizauskas, Erna Gevondyan, Parth Patel, Mohit Shekhar, Hao Wu

# Summary

---

- Our solution is focused on the protection of the user data
- Once user personal data gets into the wrong hands, the consequences can be disastrous:
  - Bank accounts, Browser logins, Contact information
- As the main focus in our solution, we propose to add an extra layer of security to the user apps

# User Needs & Specifications

---

- We designed a survey to better understand user needs
  - 63 responses
- According to our data, 65% of responders are most concerned with the security of their **data**
  - However, 68% indicated they won't take extra security measures
- We are targeting those who want an advanced data security solution.

## Alternatives & Criteria

---

- We looked at other possible solutions, such as:
  - System-wide encryption
  - Encrypted cloud backups
  - Time sensitive data destruction
  - Security for switching phone states
- However, we ran into several loopholes while exploring each of the above solutions

# Concept Description

---

- Data protection today consists of unlocking phone
  - Phone PIN lock, pattern, or face recognition
- A single barrier can be easily compromised
- Our solution involves adding a 2 Factor Authentication system for individual apps
  - Regular password + generated password from another device
    - Bluetooth keychain device to retrieve 2FA code
      - Or use Google Authenticator App

# Concept Description

---

- Solution
  - Keep the PIN
  - Add 2 Factor Authentication for individual apps
    - Regular password + generated password from another device
    - For any app on your phone you feel needs extra security
    - Use a bluetooth keychain device to retrieve 2FA code or use a Google Authenticator App

# Scenario

---

- Leave phone on desk
- Someone quickly picks it up
- PIN code is compromised
  - Guesses code, sees you enter code, or looks at fingerprints on phone for patterns
- Steals your data (& your phone)
  - *Having 2FA on the important apps is going to make it astronomically difficult to unlock them*

# Stakeholder Value Propositions

---

- Operating system developer
  - Makes for a more secure system
  - More marketable to enterprise
- User of phone
  - Sensitive data is kept safe
- Thief of phone
  - None

# Implementation Guidance

---

- We can develop the system functionality for 2 Factor Authentication for apps.
- This functionality can be appended to the open source Android operating system

## **Business Model**

---

- License Cryptone to Google and other phone operating system developers

## Risks/Mitigations

---

- Someone can break the 2FA algorithm
  - Though nearly impossible at this point in time, provided that it is implemented properly

# PRISM

Personal wrist-mounted Information Storage Monitor

IIT IPRO Team T5B

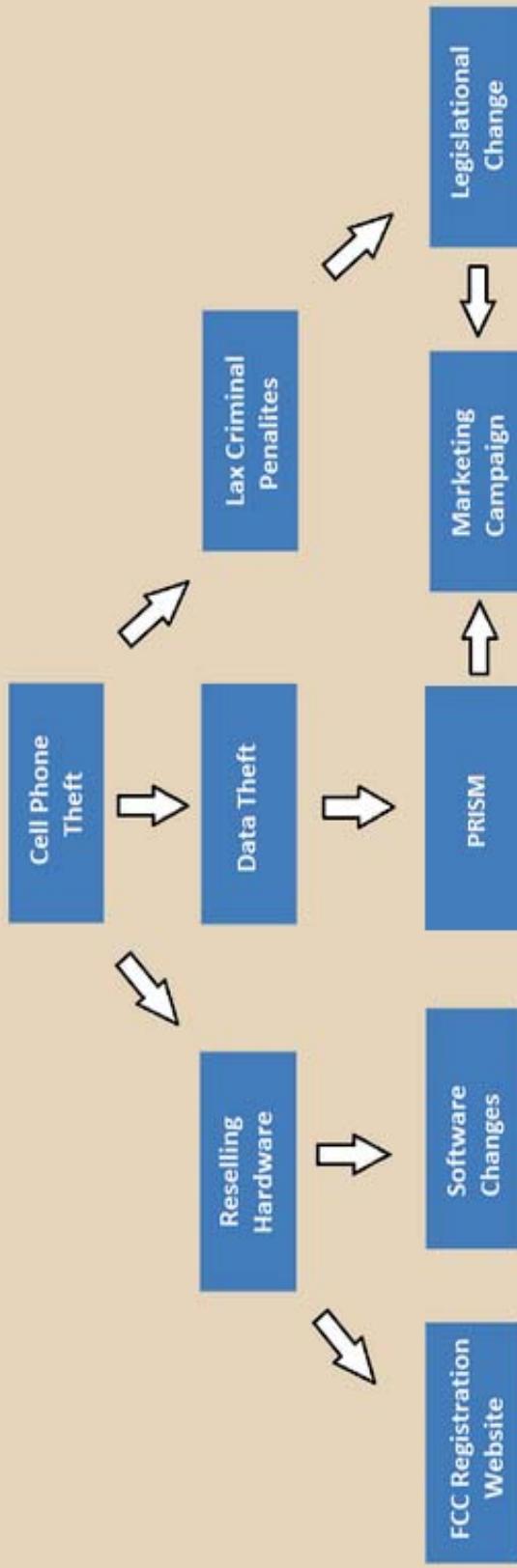
Jacob Kisiel, Austin Boos, Raj Desai, Mariana Vieira

# Need Statements

- Prevent Theft of Personal Information
- Prevent Physical Theft of Phone
- Deter Advantages of Theft
- Notify User and Related Parties of Theft
- Independent of Normal Phone Function

# Overview: Outline of Solution

Creating Countermeasures Against the Benefits of Phone Theft



# Personal Phone Monitor

- Wearable
- Distance Sensor
  - Automatically deploys safeguards
  - Easily undoable by user
- Off-Device Data Storage
  - Prevents data-theft
    - can wipe data off stolen device without completely erasing data
    - No noticeable difference to user

## Personal Phone Monitor (Pt. 2)

- Alerts
  - Notifies user of automated actions
  - Communicates with anti-theft website
  - Prevent abuse of compromised data
    - Logs physical info on phone
    - Undoable if false report

## Software

- Personal GPS
  - Distance controlled location tracking
  - Only available to phone owner
  - owner can push data to anti-theft website
- Prevent safety device disabling
  - Password protected airplane mode
  - Password protected shut-off
  - Distance controlled data-lock

# Legal/Governmental

## The Theft Report Website

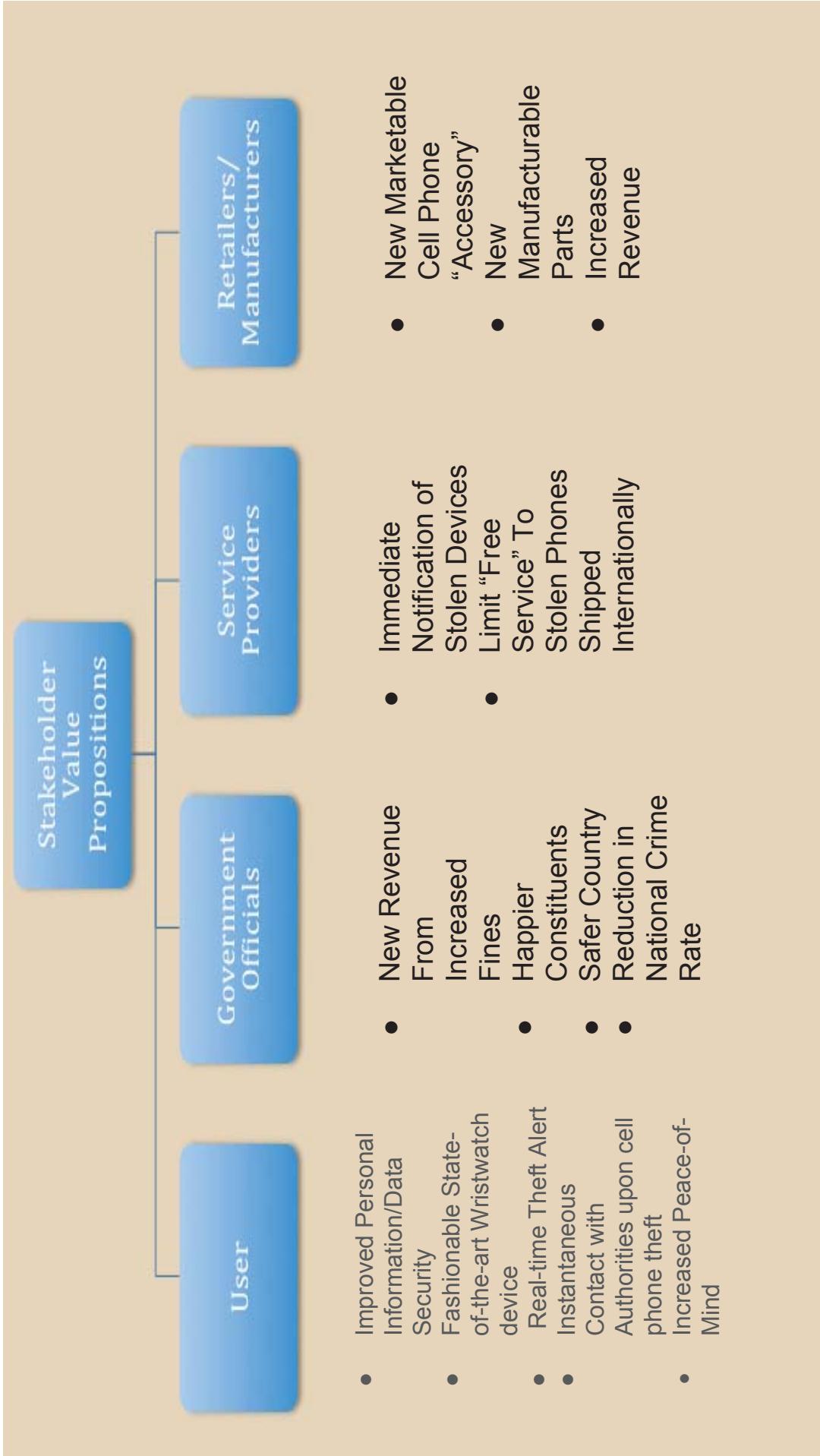
- Reduce trade of illegal phones
- Ensure phone buyers of authenticity of phones

## Harsher fines

- Discourage phone theft

## Awareness campaign

- Educate masses on the importance of being careful and alert in order to reduce the risk of their lives and the loss of material goods
- Make people aware of harsher fines
- Spread understanding of report website



# Implementation/Summary

- Software development
- Implement existent hardware (GPS, Personal Cloud) to the new product
- Manufacturing and marketing of watch (Other options - Card, Necklace, Bracelet, Belt buckle)
- Explain and educate people about how to use the product
- Make the companies aware that if the theft occur they will be notified and the necessary actions will be required (Auto-alert)
- Development of harsher fines against phone theft
- The Theft Report Website: make people and companies aware of this new tool and encourage theft report

# Chain Reaction

Presented by:

Zeming Yang, Shane Pung, Minwoo Kang,  
Tehlyr Kellogg, and Landi Gu

IIT IPRO Team T6A

## Summary

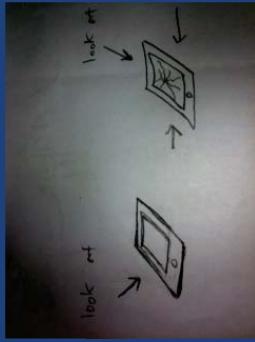
Our solution for the prevention of phone theft involves looking at every step of the theft process. We believe that improving things in each phase of the theft process will be the most beneficial for stakeholders.

# Summary

- Prevention of Cell Phone Theft
- Moment of Theft
- After Phone is Out of Reach
- After Airplane Mode or Power Off
- After being stolen and unlikely to be recover (self-destroy)
- Government Policy

# Prevention of Cell Phone Theft

- Screen protect film(Fake broken glass)
  - fake image appears at any distortion angle
  - protect personal privacy (cf. texting and facebook)
- Information protect (i-Cloud)
  - All information is updated automatically to web database even without wifi or internet
  - personal data is easy to recover
- Reduce of cost of cell phones
  - make a cheaper version of cell phone



Source: team analysis

Source: team analysis

## Moment of Theft

### Remote which activates

- high pitched sound
- camera and audio functions of phone

### Magnetic clasp

- allows owner to feel when phone is being pulled away

Source: team analysis

## After Phone is Out of Reach

- Airplane mode / Power off password
- Remote software wipe
- Remote bricking

Source: team analysis

# After Airplane Mode or Power Off

- Backup chip
- Remote kill switch
- Cell phone can receive remote signal to destroy hardware such as CPU and battery.
- everyone has an account on website. When he/she finds that the phone is stolen, he/she can brick the phone on website. Also he/she can clear all software from the website.

Source: team analysis

# After being stolen and unlikely to be recover (self-destroy)

## **Hardware**

- Reactivation of Cell phone parts
- Memory card self-destroying

## **Software**

- All data will be automatically wiped out if rooting is attempted.
- A registration of the phone to an internet program which can remove all user data.
- PD's DB tracking location of lost phone

# Government Policy

- the government should make a new law that stealing phone is a serious crime and the thief will be imprisoned for ten years.

Source: team analysis

## Risks

- Possibly too broad
- Overwhelm consumer with many precautions

# virtual—leash

michael corless  
odilon guzman-cooss

IIT IPRO Team T6B

james panek  
diego vega

*Fact:*

**3,000,000+**

*phones were stolen last year  
up from 1,600,000 the year before*

**why?**

*Fact:*

we have been carrying around small highly valuable objects for much longer a time than smart phones have been around.



Welcome To:

# *virtual* leash



through the introduction of hardware chips in the form of credit cards and key fobs, virtual leash offers three methods of protection:

- | prevents you from getting too far from your device
- | monitors your normal locations
- | protects your data without destroying it

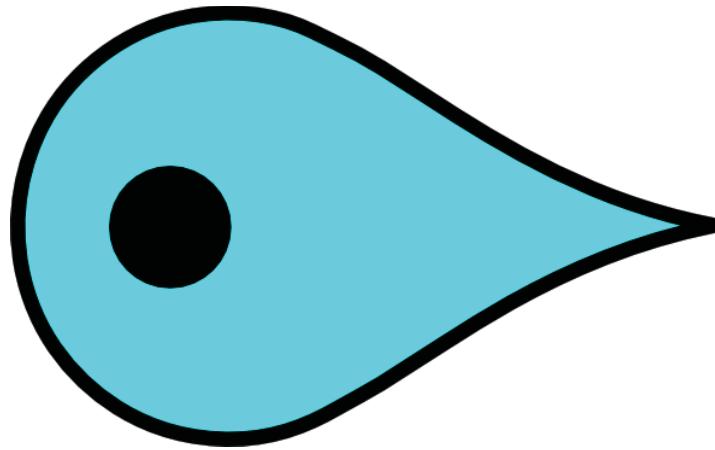


## *Rule 1:* **stay close**

- | the best way to prevent phone theft is to make sure you know where your phone is at all times
- | if one of the hardware chips is farther away than the leash is set the remaining devices will alert you through vibrations or audible signals

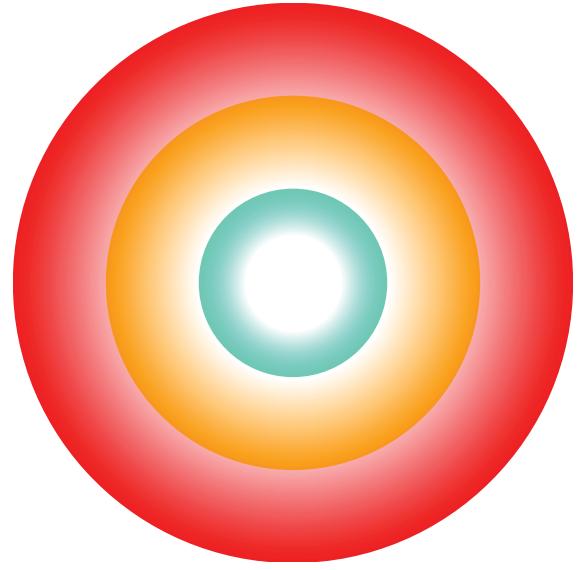


## *Rule 2:* **monitor**



- | in the same way that phones already do, virtual leash will be able to determine patterns in your daily activity detect safe zones
- | inside these safe zones, such as work and home the leash will be loosened to allow for mobility
- | outside of these safe zones virtual leash will tighten to several feet away from the other devices
- | in areas where connection to your service provider is lost, virtual leash will enter high alert mode

## *Rule 3:* **protect**

- 
- | virtual leash will use three levels of protection to ensure your data is secure
  - | if your device is removed from the first zone the other devices respond with vibrations and audible signals
  - | if the second zone is broken virtual leash begins to back up your data to the cloud
  - | outside of zone three your phone powers down and will not turn back on until all three chips are together

# *What if ?* possibilities

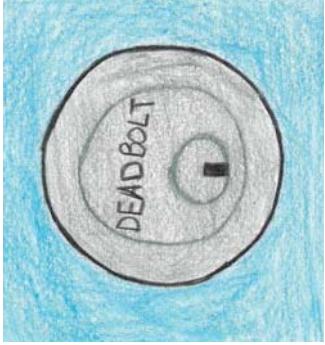
- | what if cell phone providers sold simple virtual leash chips like they do with insurance?
- | what if there were a comprehensive online interface to set preferences and increase security?
- | what if charging these devices was as easy as emptying your pockets at the end of the day?





what if?





# The Deadbolt

IIT IPRO Team W1A: Collin Dunn, Taylor Jordan,  
Jonathan Key, Nikoleta Labovic, and Javier Silva

# User Specifications

- ❖ Access to phone data
- ❖ User-intuitive solutions
- ❖ Pre-theft needs
  - Personal data protection and storage
- ❖ Post-theft needs
  - Render phone unusable
  - Incident reporting
  - Information protection
  - Device tracking



# Alternatives Considered

- ❖ Biometric security measures
  - Fingerprint/eye scanner
  - Does not provide ease of access
- ❖ Wearable proximity device
  - Not applicable when someone misplaced belongings
- ❖ Hardware destruction
  - Phone is destroyed upon theft
  - Not user intuitive as false positive may trigger
- ❖ Asking people to stop stealing phones
  - Financial incentive too great



# Summary of Idea

- ❖ Available on every smart device
- ❖ Comprehensive reporting system
  - All-in-one solution
- ❖ User-friendly security
  - Ease of access
- ❖ Computer program and app interface
  - Pre-loaded app
  - Remote access program



# Detailed Description

- ❖ GPS independent of airplane mode and main battery
  - Battery cell for GPS
  - Signal blasts every 15 minutes to locate
- ❖ Computer program with app
  - Access to disable phone features and functions
  - Reports phone as stolen
  - Also a "lost my phone" or non-emergency location feature
- ❖ Passive alerts
  - Text message alerts when in high-crime areas
  - Headphones disabled at night in high-crime areas



# Scenario of Use

- ❖ Phone stolen
- ❖ Victim accesses program to report theft with:
  - Computer
  - Text message
  - Phone call
- ❖ Victim wipes phone's data and disables functions
- ❖ Specialized law enforcement department tracks phone



# Risks/Mitigations

- ❖ Security breach of program database
- ❖ Inadequate Funding
- ❖ Implementation and development cost
- ❖ Phone carrier disapproval
- ❖ Infringement upon consumers' privacy
- ❖ Older devices not equipped
- ❖ Consumers unwilling to upgrade to new device



# Interest Groups

- ❖ Consumers
  - Safety of information
  - Peace of mind
  - Ease of use
- ❖ Carriers
  - Minimized extraneous charges
- ❖ Government
  - Boasts higher homeland security
- ❖ Device makers
  - Reduced cost of replacing phones
  - New security marketing advantage



# Business Model

- ❖ Initial investors
  - Phone companies
  - Make return on investment with moderate phone price increase
- ❖ Secure devices have a high demand
  - Consumers willing to pay for security
- ❖ Job creation
  - Security development
  - Specialized law enforcement department
- ❖ Demand for security will only increase



# Steps of Implementation

- ❖ Program development
- ❖ Device maker incorporation
- ❖ Carrier approval and incorporation
- ❖ Sample case testing
- ❖ Advertisement and phone theft education
- ❖ Full-society incorporation



# The **Excommunicator**

IIT PRO Team W1B: Deion DeBoise,  
Maimuna Venzant, Wei Li, Eunice  
Rodriguez, Matthew

# What is it?

Separate device

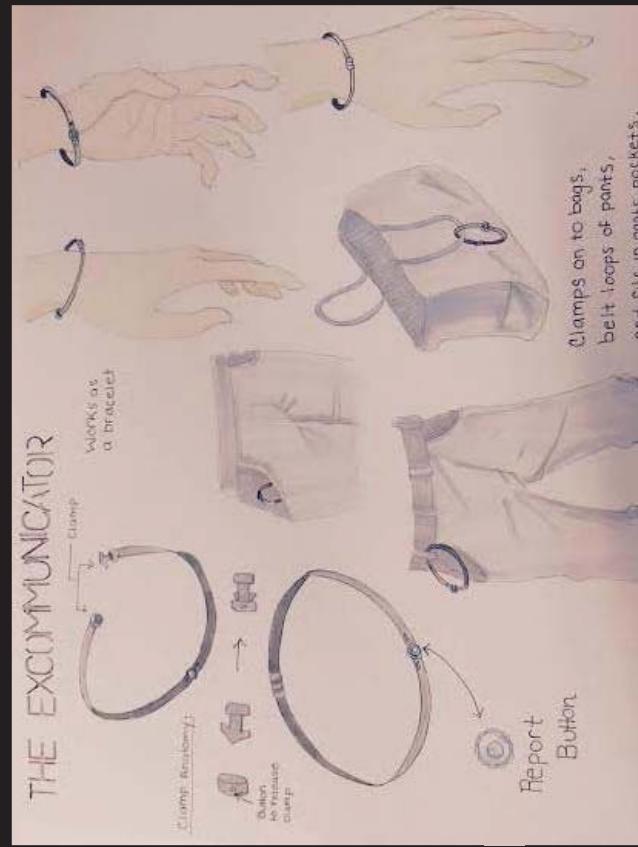
-Phone locator

-Automatic contact device

-Phone Disabler

-Acts as a bracelet, and also clamps on to pants and bags.

- Vibrates automatically when bluetooth on the phone loses range from the device, to warn the user when they forget their phone -Airplane mode locks when device is not near the phone, so thief cannot turn airplane mode



# User Needs / Specifications

Simple, small, and lightweight device/ easy to use  
Portable device: bracelet/ clip on  
Notification system:

Phone needs to be less forgettable-

Warn the user when they are a certain distance away from the phone by a strong vibration

Contact the phone company easily

Keep thief from using the user's phone:  
device will not unlock for thief when device is not near the phone

# Alternatives

## Design Criteria

- Easy to use
- Wireless automatic contact
- Make smart device harder to forget
- Does not endanger or call attention to consumer

## Initial Concepts

- Jewelry that notifies you when it is left behind
- Smart device cases that impede theft
- Add-ons that alert a third party when a device has been stolen
- Weapon add-ons to a smart device the consumer can use against a potential thief

# The Technology

The Excommunicator will contain the following:

- Small Bluetooth (Example: BlueCore BC7830 Wireless Single Chip Solution)
  -   
<http://www.csrlabs.com/bluecore7/bluecore7-wireless-single-chip-solution/>  
Small Body penny and boats to types of technology
  - Plastic / Carbon Fiber (longer lasting)
  - Custom Battery
    - Would need to be small and mostly flat (possible coin cell battery)

# Scenario of Use

## Theft

- Phone can't be turned off or put on airplane mode without device.
  1. Gunpoint
    - a. Phone will be taken but will not unlock without device nearby.
    - b. Periodically prompt owner if device is not nearby. Will contact appropriate people to report stolen if ignored.
  2. Snatched or Pick Pocketed
    - a. Notify that phone is out of range.
    - b. Phone locks and will require passcode to temporarily unlock. Calls appropriate people to report itself stolen if ignored.

## Forgotten

- Device will vibrate when phone is out range. Phone receives notification of device out of range as bluetooth connection will be lost
- This device will standardize tracking and contacting the correct parties

# Stakeholder Value

## Phone Manufacturers

- Customer Satisfaction, Build faith in their brand
- Service Providers
- Less fraudulent use of phone overseas
- Less insurance claims on stolen phones
- Build faith in the service resulting in longer lasting consumership

## Consumers

- Reduces likelihood of losing or getting their phone stolen
- Saves money by not needing to buy replacement phone.

## Government

- Less complaints from the user
- Protection of consumer privacy/ personal information

# Business Model

## Key Partner:

- Phone Distributors, Phone Manufacturers, Phone Services Resources

- Bluetooth Chips, plastic provider, battery manufacturers

## Customers

- Phone buyers

## Cost Breakdown

- This would be an add-on item
  - Bluetooth: \$6.00 (estimate from general bluetooth chips), Plastic: \$2.00 per pound (estimated from general plastic use), Custom battery: no estimate for this (depends on the technology)

# Risks/ Mitigation

## Risks

- False alarm
  - When the phone company calls the owner, the owner will have to let them know it's a false alarm before they deactivate the phone
- Forgetting device
  - Phone will automatically buzz and warn you that you are not near your device before you leave without it
  - Phone company will automatically call your phone, and owner must let the phone company know that they forgot their device

## Mitigation

- Use GPS location to deactivate the device at specified locations.
- Report button only reports when pressed twice in rapid succession.

# Implementation

## Advertise with phone purchases

- cheaper prices with contract
- prevention option
- allow phone discount or future phone discounts with purchase of this item

## Allow for customization

- several different colors or materials
- come as difference accessories such as necklace or wristband

## Demonstrate Possibilities

- Demo of what the product can do
- Emphasize other functionality such as the reminder when your phone is not nearby

# Bio-optic Anti-theft System

IIT IPRO Team W2A

Bobbie Bowman

Alex Buoscio

Michael Miszczak

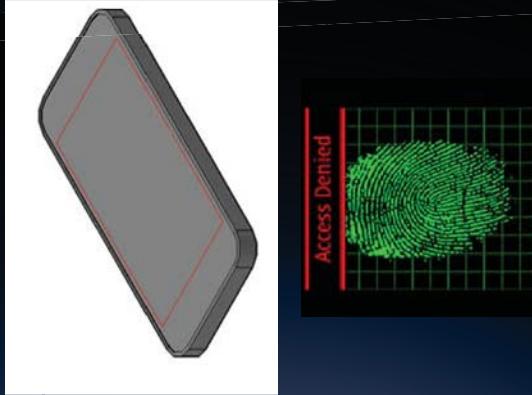
Haripriya Pandya

Sohail Noor

# Summary

Our group came up with many ideas and were finally able to incorporate a combination of functions into one device proposal, including:

- Back up Battery
  - Retina Detection to Unlock phone
  - Fingerprint detection for SIM Removal
  - Combination lock for Battery Removal
- These abilities work together to optimize the security of the user's device.



-[https://lh6.ggpht.com/cDelMkdJUUjqZcvbcd2AN3FFbiuedRJ-FYp6KTrvfsAeG9ANmey\\_nPBFR\\_V2XXXHSHGX=w300](https://lh6.ggpht.com/cDelMkdJUUjqZcvbcd2AN3FFbiuedRJ-FYp6KTrvfsAeG9ANmey_nPBFR_V2XXXHSHGX=w300)  
-Phone concept design from Team W2A.

# Goals

- Prevent phone theft
- Prevent identity theft and crimes related to identity theft
- Reduce tax frauds
- Reduce bank and credit card frauds
- Increase security on streets and decrease the fatality due to phone thefts
- Spread awareness about phone theft and issues related to it

# Product Functions

The consumer needs:

- To be able to track phone
- To be able to retrieve phone
- To be able to secure phone
- Phone must be affordable

Specifications

•Phone must have a tracking device

•Phone must have better security features

•Phone must be affordable and available to consumer

-<http://hikinglady.com/wp-content/uploads/2009/12/Outdoor-GPS-Unit1-e126679970649.jpg>

-<http://dinogiacomazzi.com/wp-content/uploads/2012/03/Smartphone-security.jpg>



# Alternatives

We considered implementing:

- ❖ Voice activation
- ❖ Tether systems
- ❖ Bluetooth abilities

Looking at these systems, we realized that voice activation will not work if the microphone is damaged or covered, or if the user has a cold or has lost their voice.

If the phone is tied to the user, it can restrict mobility, or cause damage if snagged on a branch.

Bluetooth has a very small operational range, and won't help track a device over long distances.

These criteria were not good, so narrowing down our pool of ideas to make a phone that had both physical (hardware) and virtual (software) abilities to track and lock/secure the phone were chosen.

-Blu <http://media2.giga.de/2012/01/Bluetooth2.jpg>  
-<http://www.e-commercefacts.com/news/2012/01/siri-for-e-commerce/siri.bmp>  
<http://gearkeeeperblog.com/wp-content/uploads/2010/12/phone-tether.jpg>



# PROCESS

- The fingerprint lock system and combination lock on the back cover prevents thieves from using the loophole of turning off the phone to disable the GPS. This way the phone can be tracked even after being stolen
- The use of the backup battery will keep the GPS on for a lengthy period even in the case of the phone running out of regular battery
  - The use of retina detection prevents thieves from stealing important personal information as phone can not be unlocked
- The encryption of the SIM card through either a PIN or a fingerprint for the safety of contacts gives more protection to identities.



# Stakeholder Value

- Consumers are guaranteed to recover their phone with all devices in place along with the physical lock
- Device makers will be able to increase the sales for smartphones worldwide with the extra security to quickly find and retrieve the smartphone
- Makes it easier for law enforcement to find thieves and create a disincentive for stealing smartphones
- Reduce the probability of carriers giving thieves free access to phone lines overseas and with more smartphones being used overseas, more money will be made by the carriers

# Business Model

- Attracts more users due to enhanced security
- Use of biometric locks has passed testing phase and now in commercial usage
- Due to increased security and decreased insurance, phone sales are highly likely to increase
- Slightly increased cost due to additional features although no need of extra accessories
- Increased security of the smartphones will attract customers globally
- Increased safety for consumers due to decreased possibility of attempts to apprehend thieves

Phone concept design from Team W2A.



# Risks and Mitigations

The risk our model possesses include:

- The physical appearance of the combination lock (consumers might like the design of the phone more than the security features it has to offer)
- There is always a chance that the users may not like the phone, software, or its security system (Some People prefer to have a name brand Phone Like the iPhone, or Android)
- Component failures (hardware and software)
- Biometrics won't function for people with Physical limitations (Prosthetic hand, or artificial eyes)

Mitigation of risks:

- Market the phone as “The most secure phone on the market,”
- Quality control and testing for device
- Have multiple systems in place (someone with a prosthetic hand can opt to use retinal scan for allowing phone access and vice versa)

# Implementation

- ◆ Design the device, and its internal architecture
- ◆ Create a company to manufacture new device.
- ◆ Field test the device and its functions.
- ◆ Offer free trials to gain initial consumer base
- ◆ Market to the consumer as “The securest phone on the market”

Back panel  
lock



[https://www.google.com/url?sa=i&cte=ieo&src=s&source=images&cd=&docid=pdM3DX5SB-7aYM&lnrid=mma7napD02kKhM&ved=0CAQQIBw&uri=http%3A%2F%2Fupload.eovv.com%2Fupload%2FProduct%2F200911%2Fchina\\_silver\\_3\\_number\\_alloy\\_lock200911202102326.ipdte=IMQkVJnukKdhB8QG\\_dde=MQkVJnukKdhB8QG\\_psig=AfQICNHiHmIawcgbMOJq6Ba22G8oyNtR2w&usl=141178215968243](https://www.google.com/url?sa=i&cte=ieo&src=s&source=images&cd=&docid=pdM3DX5SB-7aYM&lnrid=mma7napD02kKhM&ved=0CAQQIBw&uri=http%3A%2F%2Fupload.eovv.com%2Fupload%2FProduct%2F200911%2Fchina_silver_3_number_alloy_lock200911202102326.ipdte=IMQkVJnukKdhB8QG_dde=MQkVJnukKdhB8QG_psig=AfQICNHiHmIawcgbMOJq6Ba22G8oyNtR2w&usl=141178215968243)

Phone concept design from Team W2A.

# LifeBoard + LiferRing

IIT IPRO Team W2B: Mitchlie Martyr, Patryk Walos,  
Sneha Gindodiya, Jacob Mansfield, Emma Zachocki

# Summary of Concept

How Will It Solve  
the Problem?

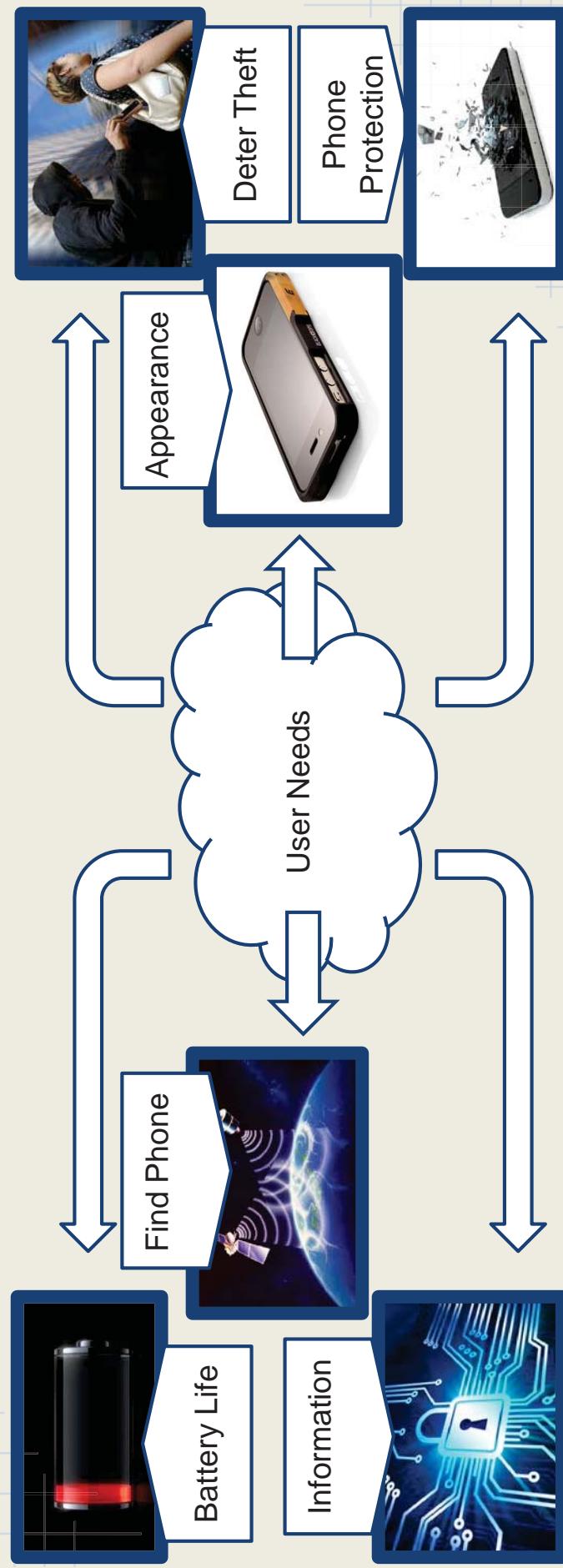
Phone thieves will be less  
likely to steal a phone with  
this product due to it's ability  
to help catch the thief

LifeBoard  
LifeRing

How Does It  
Work?

- It is a phone protection system that uses an app, watch and phone case
- When the case and watch are too far away:
  - Phone case goes into 'panic mode'
  - Phone goes into 'theft safety mode'

# Assessment of User Needs



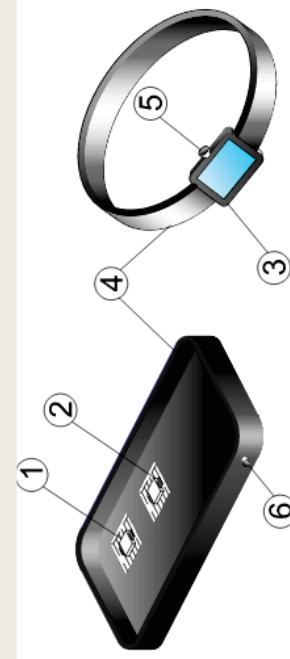
Picture reference: [http://www.destinationrewards.com/images/blog/201209271523321406\\_092612blogimage.jpg](http://www.destinationrewards.com/images/blog/201209271523321406_092612blogimage.jpg) , <http://www.thesiar.com.nv/~media/Images/TSOI/Photos-Gallery/Nation2013/08/02/phone%20theft.aspx?w=620&h=413&crop=1&http://www.smartofosecurity.com/wp-content/uploads/GPS-Tracking-Systems.jpg> , <http://www.wired.com/wp-content/uploads/2011/11/case.jpg>, <http://www.gadgetreview.com/wp-content/uploads/2013/04/original2-650x365.jpg>, <http://www.aussiebatt.com/blog/wp-content/uploads/2013/01/cell-phone-battery-life.jpg>

# Alternatives Considered

- Waistband tether line that keeps phone secured to body
- Cell phone emergency hotline
- Remotely destructible internal parts
- Public safety announcement
- Requires biometrics to allow use of phone
- Phone that releases a neurotoxin
- Taser phone

# Detailed Concept Description

- Phone Case<->Wristband Combination
  - LifeBoard features
    - physically locks to phone
    - connects to phone through micro usb/apple lightning
    - its own battery power source
    - gps location chip
    - bluetooth chip
    - speaker for alarm
    - waterproof
  - LifeRing features
    - bluetooth chip
    - small speaker
    - lithium ion battery
    - micro usb port
    - panic button
    - LCD screen
    - clock
- The **LifeBoard** attaches to the phone and can only be removed with a physical key. When the case is 10 feet away from the **LifeRing** the LCD screen asks if the user would like to activate “panic mode”. While in panic mode, **LifeBoard** blares an alarm, notifies the service provider that the phone has potentially been stolen, sends gps locations to the carrier, and uses the phone’s camera to periodically take photos and sends them to the owner’s email.



**LifeBoard**      **LifeRing**

1. Dedicated GPS Battery built into LifeBoard
2. Dedicated Panic Button Battery
3. LCD Screen to Monitor LifeBoard
4. Integral link between LifeBoard and LifeRing
5. Panic Button on LifeRing linked to LifeBoard
6. Panic Button on LifeBoard linked to LifeRing

# Scenario of Use

1. Phone is stolen and the **LifeRing** beeps to alert the user
2. User is asked to put phone into panic mode
3. Phone locks down and prevents the phone from being put into airplane mode.
4. Phone can only be taken out of airplane mode by user entering his or her specific pin.
5. **LifeBoard** starts blaring an alarm.
6. Service provider is notified and receives gps locations
7. Phone periodically takes photos and sends them to the users email account
8. Hopefully these combined efforts with the police can relocate and return the stolen phone

# Stakeholder Value Propositions

## Consumers

- Save money on not having to replace stolen phone
- Extended battery life
- Extra security
- Extra physical phone protection
- Clock on wristband

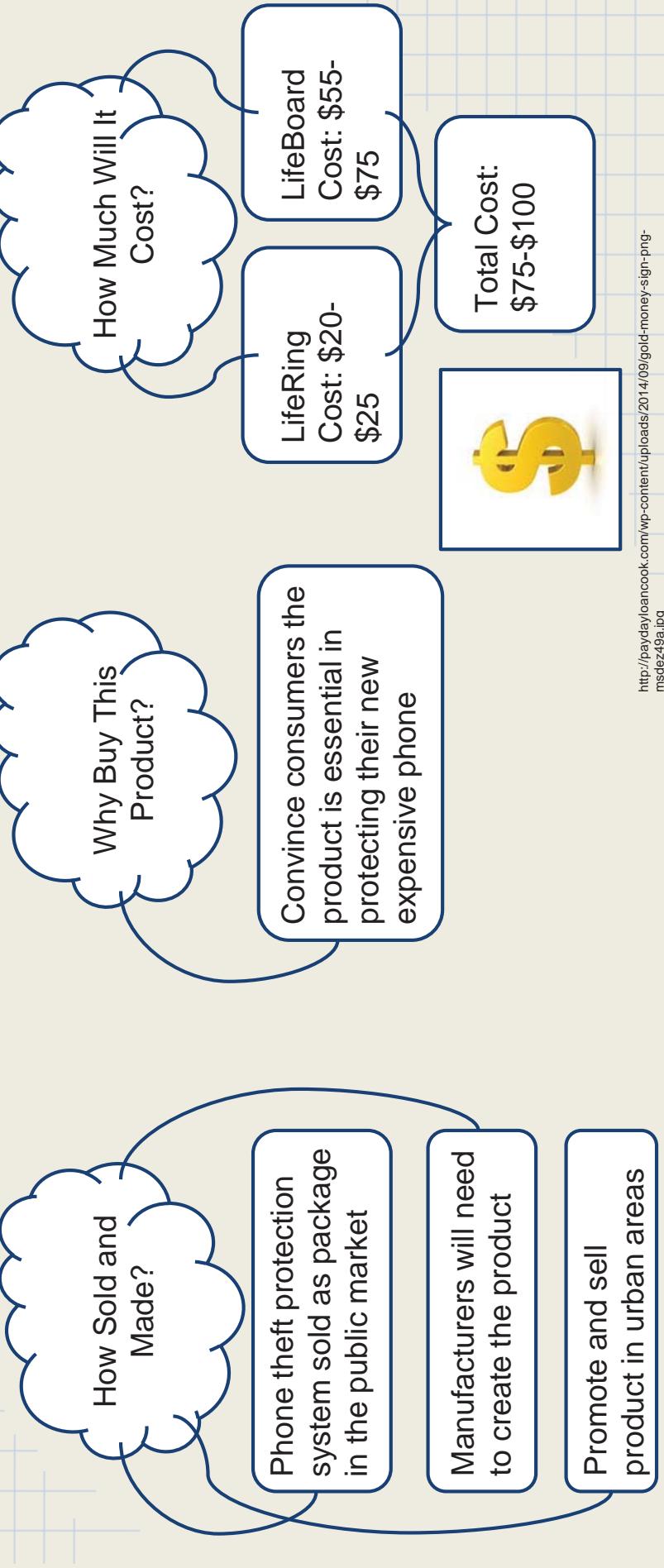
## Carriers

- Save money on replacing stolen phones
- Charge for extra protection services
- Sell the product in stores

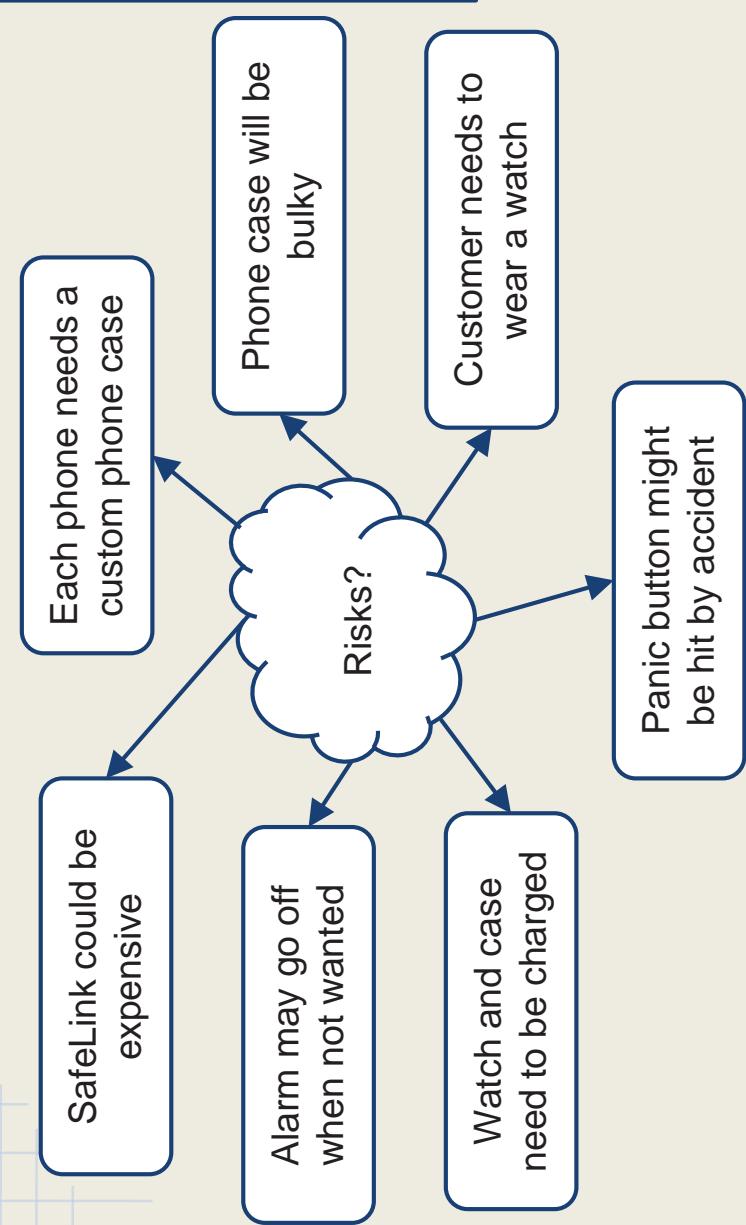
## Manufacturers

- Make and sell product for a profit

# Business Model



# Risks / Mitigations



# Implementation Guidance

Customer Ease Of Use

Physically, the customer just needs to put on the watch and case

- App Installation
1. Download app
  2. Connect phone and case with app
  3. Customize setting

World Implementation

Give idea to manufacturers

Government does not need to be involved

Carriers will push for customers to use SafeLink

How Effective Is This Implementation?

Could prevent at least a small portion of phone theft each year

This idea will not solve the whole problem of phone theft but it is a good idea for some specific consumers

# Phone Prevention

IIT IPRO Team W3A  
Shacara Ledbetter  
Jeremiah Nelson  
Monica Patel  
Cesar Sanabria  
Sarah Williams

# User Needs

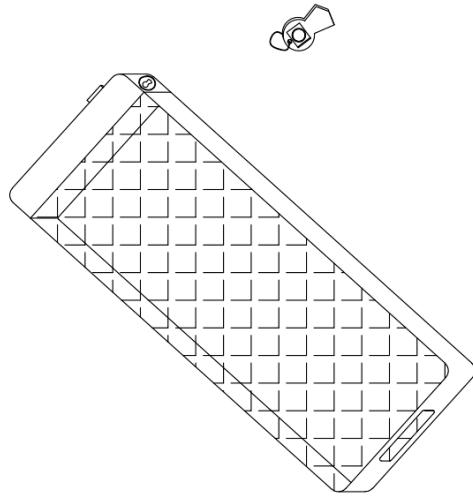
- According to Lookout Mobile Security, about 50% of phone theft victims would pay \$500 to get their devices back. One-third of victims would pay \$1,000 to retrieve their stolen smart phones.
- Users stated that they needed:
  - Data Security / Recovery
  - A way to prevent theft
  - A way to recover device
  - Personal Safety

# Step 1

- Phone prevention step. This is the step where the customer buys a product to make the phone more secure. There is a specialized case with its own unique key/ panic button.

Purchased product will include: A case, key, panic button.

The case will be able to secure the device in order to prevent the battery and sim card from being removed. The key will be used to remove the case. The key will include and panic button.



# Step 2

- Phone is stolen.
  - In the event that the phone is stolen, It will require a password in order for the phone to be turned off and on. A password will also be required to turn the phone into airplane mode

# Step 3

## ► Retrieving lost or stolen device.

- The device will included a second internal battery for built in tracking purposes only. The device will take a photo and send a gps location to the users email. Also the location history will be accessible through and application

# Step 4

- information protection.
- All information can be added and deleted through a secure program
- An application that comes with the device will be paired with a computer. In the event that the phone is stolen, it will be possible to add and delete all files on the device via computer.

# Step 5

- The virus is hardcoded into the device. The virus can be activated by username and password. The virus will delete all the files on the computer and make the phone useless.

# Risk

- ▶ High financial cost “production, and maintenance”.
- ▶ Lack of technical support.
- ▶ Faulty software/ programming code.
- ▶ Faulty case design, which could lead to more financial problems.
- ▶ Security key can be potentially misplaced or lost.
- ▶ Finding responsible partners, who can help modify and finalize the final product.
- ▶ Total system breakdown from potential hackers.
- ▶ Severe breakdown.
- ▶ The finances might outweigh the overall goal.
- ▶ Our inability to globalize this security system.

# Business Model

- The case and key needs to be of alloy metal for strength, resist corrosion, act as a protective case, as well as have an appealing appearance with low cost.
  - Stainless steel the most effective in terms of corrosion resistance, as well as maintaining a clean appearance. This is also a strong metal alloy that is hard enough and has enough tensile strength to resist tampering.
- Other costs will include the man hours needed to effectively resolve the situation as well as software needed.
- Funding can come from the carriers, or accessory companies themselves if not the government; since this is an issue of governmental concern.

# Stakeholder Value

- There is stakeholder value in this solution for consumers, carriers, the government and the device makers via resolution by product consumption. This solution reduces the need for actual man power to prevent phone theft and could generate another source of income for the accessory company and phone companies by selling this product. It is as the consumer's discretion to take the necessary steps for prevention. The situation is deduced to the consumer prioritizing the importance of the device and the information it holds.

# Implementation

Since we addressed the problem through a series of steps, it makes sense to implement the solution in steps as well.

- ▶ Step 1 : Develop phone case and key with an existing phone accessory company and partner with service providers to sell in their stores.
  - ▶ Step 2: Work with phone manufacturers to add additional security elements to their phones, including additional password protections, a second internal battery, and also the “virus” that can erase information if the phone is unrecoverable.
  - ▶ Step 3: Develop application(s) to monitor attempts at unlocking the phone, record device location history, and control data stored on the phone. Look into marketing these applications to service providers to use as a default application upon purchase.
- To implement these ideas cooperation of the cellular service providers as well as phone manufacturers would be needed. Their incentive is the ability to market phones that are less susceptible to unauthorized access and more easily recoverable in the case of theft.
- 

# G-LOCK

with password protect.

Eritomiwa Sobayo  
Matthew Ross  
Jeremy Tapia  
Allen White  
Freddy Herrera

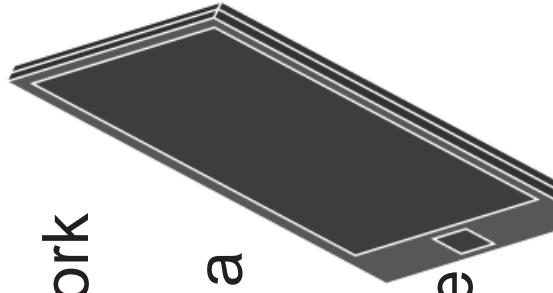
IIT IPRO  
Team W3B

A Gear Locked (G-Lock) phone can not be taken apart or be connected to a USB charger. Password Protect sends you info about who's trying to open your phone.

# Assessment of User Needs

---

- Discourages the theft of phones
- Discourages the use of stolen phones
- Makes selling a stolen phone harder
- Makes it impossible to take the phone off a network through a physical connection (usb cord).
- Makes it impossible to hack a password through a physical connection (usb cord).
- Provides the user a photo of the culprit and their location after unsuccessful attempts to unlock the phone.



Sample Phone design made in Microsoft Word.

# Alternatives Considered

---

- Remote access that can be used to make the phone overheat and render it useless.
  - Problem with this is that there is no chance the phone will have any use if recovered.
- Automatic Police Dept. Calls Upon incorrect password entry.
  - Accidental entries or childish pranks will waste even more of police resources.
- Constant GPS signal tracking
  - Issues with privacy and the information being used for malicious purposes.

# Concept Description

---

## G-Lock:

- Physical locks bind the phone's back to main components (if the back is forced off all useful components of the phone will be destroyed)
- Physical cover prevents the phone from being charged or being physically connected to a PC.
- Can only be unlocked via a password (no external unlocking or override exists)



Back of phone (inside view) made in Microsoft Word.



Phone (inside view) made in Microsoft Word.

# Concept Description

---

- Password Protect: When either the phone's password or the G-lock password has been entered incorrectly too many times.
  - A selfie of the culprit will be taken and sent to the an email set up by the user.
  - The phones location and information will be sent to the email and the service provider.



Sample Phone (top view) made in Microsoft word.

# Implementation Guidance

---

- Making the public Aware of G-lock:
  - Making sure people know to keep their phone G-Lock at all times (except when charging it)
  - Making sure thieves know that stealing a G-Lock phone is a wasted effort because it's inaccessible and worthless to anyone without the password.
- Teaching users about Password Protect and providing instructions on how to set up an account for the selfies.
- Service providers need to keep a log of locations sent to them by Password Protect incase the phone is reported stolen.

# Scenario of Use

Claire was walking home from the beach alone at 9pm. She has a brand new phone in her hand when a hooded stranger jumped out of the bushes and takes her phone. Luckily for Claire her new phone was G-locked.

Now as the hooded stranger tries to unlock the phone with his PC he finds that he can't because the charger has a cover on it. Also because he can't get into the phone, he can't take it off the network. Now he tries to guess her password a couple of times. ↓

Thanks to Password Protect a selfie and location info was sent to claire and her service provider. The stranger was picked up by the police a few hours later and claire was able to recover the phone, with all her information untouched.

# Risks / Mitigations

---

- Hardware failure can result permanent lock and a useless phone.
  - Warning users and informing them to handle phones delicately can reduce chances of hardware failure.
- It is impossible to un G-Lock or charge a G-locked phone whose battery is completely dead.
  - Reserving a portion of the battery energy or having a back up battery specifically for G-lock will ensure the phone can always be unlocked.

# **Business Model**

---

- Phone manufacturers will be responsible for new phone with G-Lock and Password Protect.
  - Password protect is all software and G-Lock only requires small physical locks, software and possibly a small secondary battery. Meaning material cost will be minimal.
- Other cost may occur if the locks malfunction or the thief forces the phone open and breaks it. Requiring a replacement phone (since the old one is now useless). This cost may fall on the user, service provider or phone manufacturer, depending on contracts.

# Stakeholders - Value Propositions

---

## Mobile Device Owners

**For:** Owners of costly mobile devices

**What:** Need to feel that they and their belongings are protected.

**We provide:** Peace of mind with the implementation of the G-Lock

**That:** Lowers the probability of theft and protects information in the event of theft.

**Unlike:** Other companies that have few measures in place.

**We:** Are dedicated to your security

## Mobile Device Companies

**For:** Companies who sell mobile Devices.

**What:** Need a way to decrease the wave of thefts related to their products.

**We provide:** A Cost effective solution to the problem of theft

**That:** That will distance their products from the devaluing effects of theft.

**Unlike:** Services like apple care that do not work to solve the problem but instead to generate more revenue.

**We:** Are motivated by solutions that revolutionize the mobile device industry.

---

# FCCC Phone Security Project

## IIT IPRO Team W4A

Kapil Vyas

Yaw Asare

Jessica Castro

Adrew

Jacob Ochhwat

# Main Solution

- Our super phone consists of a three step solution that begins with phone theft prevention and ends with discouraging the thief from robbery.

## Step One: The Strap-IIT Strap

- The Strap-IIT solution (pronounced- Strap-it) is a set of three finger straps attached to the back of the device that the user slides his fingers into while using the device. The purpose of this is to have a better grip/hold on the device to prevent phone theft in the first place.

## Pre-Step Two and Three: B-Batt

- The second part of out solution requires a back-up battery fitted inside the device. This battery is separate from the main device battery and is used to power the emergency devices. The point of this internal battery is so that the emergency devices work despite the thief removing the main battery.

## Step two-Part 1: GPS-IIT

- The GPS-IIT solution activates after/if the phone is stolen.
- With a lower grade tech the user possesses a wristband with a button that activates the location of the phone which can be accessed through a computer or by calling the police.
- With a higher grade tech, a smart watch synced with the device can show the location of the phone on a screen.

## Step two-Part 2: Store-IIT

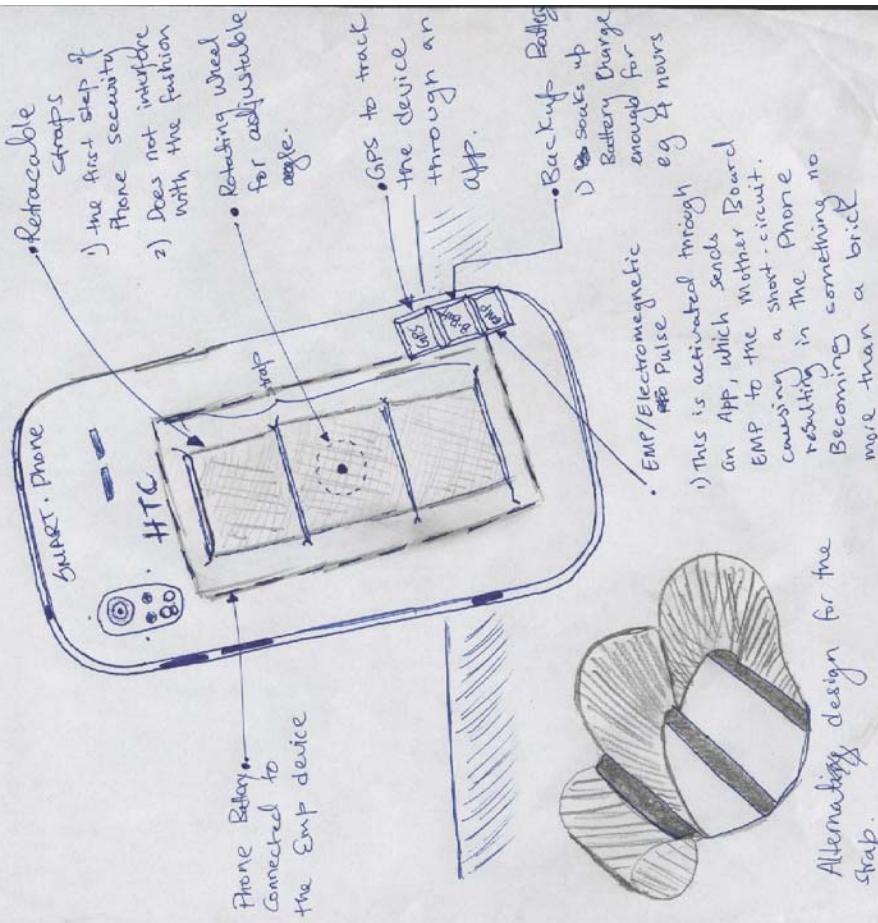
- While the user is trying to locate their device using the GPS-IIT, with hopes of still retrieving the phone, the Store-IIT is backing up and securing all the phone memory into a one way memory storage location that can be extracted at a later time with a specific access code.

### Step three: Fry-IIT

- The last and final solution is activated when all hopes of locating the phone are lost. An electromagnetic pulse (EMP) will cause electronic disturbance in a short burst of electromagnetic energy. This can be activated using the wristband or smart watch device or by calling the phone company. This pulse will cause the phone to short circuit and make it useless.
- Conclusion: This emp is used in hopes of discouraging the thief from stealing a phone that will become useless.

## Phone Security FCC Project

Main Solution: Using AN ELECTROMAGNETIC Pulse  
An Electromagnetic pulse (EMP) will cause electronic disturbance  
in a short burst of electromagnetic energy. Such a pulse may  
occur in the form of a magnetic field or conducted electrical  
current depending on the source.

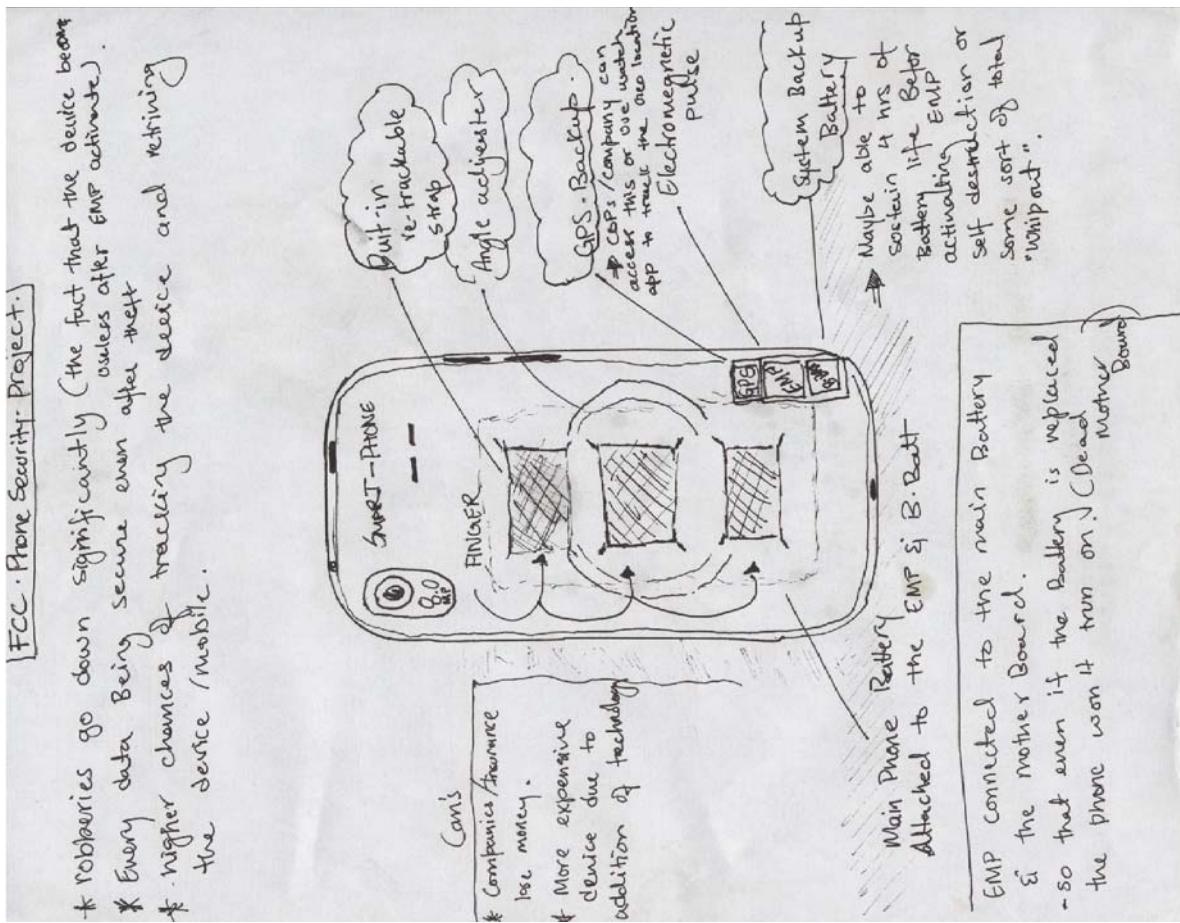


# Image 1

### FCC · Phone Security Project.

- \* robberies go down significantly (the fact that the device becomes unusable after EMP activate).
- \* Every data Being secure even after their higher chances of tracking the device and retrieving the device/mobile.

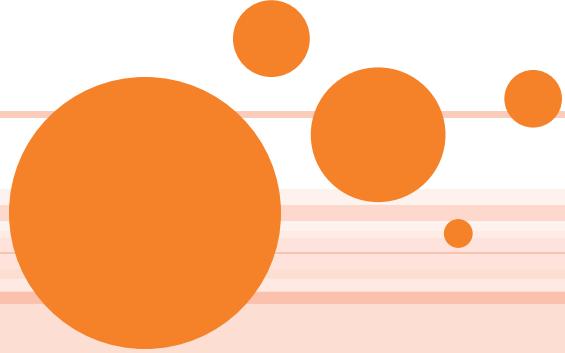
## Image 2



Julie M. Leong Chenzhiyuan Rong Konrad Sniezek  
Evan Tjondro Koesoemo Mario Velazquez

# STOLEN CELL PHONE CHALLENGE

IIPRO Team W4B



## SUMMARY

Solve the problem of phone theft by preventing it, alerting the owner and authorities as soon as the phone is stolen, being able to remotely deactivate the sim card, and being able to short circuit all components of the phone.

Make phone theft obsolete.

Monitor sim card activity.



# USER NEEDS & SPECIFICATIONS

## Protect owner and contacts

- 90% chance of no harm to owner
- 100% chance of no harm to contacts

## Stay connected with phone data

- 100% chance of recovery

## Have quick response

- 1 second

## Feel more secure about phone

- 80% people feel secure



## ALTERNATIVES

- Adding additional password requirement to place phone in airplane mode or power down
  - More hassle for consumers and does nothing to deter thieves from selling the components instead of the phone as a whole

- 5 password attempts and phone is locked and network provider is notified
  - Inconvenient for consumers and network providers

## Make phones simpler and cheaper

- Most people want fancy phones that do more



## FEATURE DETAILS

### Feature

- Each charger and device is programmed with matching IP addresses, like computers. Therefore, each phone can only be charged by its own charger.
- Phone is paired with external device (microchip in card, watch, etc.). Alarm sounds if they are separated user-specified distance and network provider is alerted.

### Scenario

- Criminal has stolen phone, but can only use it for the life of the battery. Stolen phones will have little value since they can't be charged, deterring thieves.
- Phone is stolen. After specified distance is surpassed, alarm sounds from phone and alerts surrounding area. Provider tries to contact user. If unsuccessful, then contacts police.



## FEATURE DETAILS (CONTINUED)

Feature	Scenario
<ul style="list-style-type: none"><li>User can view data (contacts list, etc.) or deactivate the sim card in order to prevent phone usage, like viewing or shutting down a credit card.</li><li>If criminal attempts to disassemble phone without authorization, when internal connection is broken, data is immediately backed up to sim card account and all components short circuit.</li></ul>	<ul style="list-style-type: none"><li>User notices missing phone and goes online to instantly deactivate the sim card without the assistance of the network provider.</li><li>Criminal can't sell phone to consumers, so attempts to sell components. These components are shorted out and useless.</li></ul>



# STAKEHOLDER VALUE PROPOSITIONS

## Consumer

- Phone insurance is cheaper
- Phone doesn't get stolen

## Carriers

- Not have to pay unauthorized usage
- No need to hire employees to deactivate phones

## Government

- Have good reputation
- Reduce tasks for police

## Device Makers

- Make and sell more components and accessories
- More customers

# BUSINESS MODEL

- Government first invests financially in such technology and in promoting it
- Phone makers create these components and ensure proper installation
- Consumers pay for these products if they desire to have such features



## RISKS/MITIGATIONS

- Losing charger will cause consumer distress
  - Need for new charger from provider
- Potential pranks gone wrong
- Potential data backup breaches
- May start trend of stealing phones just to have them destroyed.



## IMPLEMENTATION

- Initiate test trials throughout the country
- Advertise to public
- Offer limited free trials, then charge consumer
- Offer these features on new phones



# Anti-Phone Theft Solutions

**Theme:** Alert Systems

IIT IPRO Team W5A:

Alejandra Gonzalez, Andy Huang, Asbel Assefa, XingYu Liang

October 1, 2014

# STATS and FACTS

Jon, a careless teenager has fallen victim to phone theft after forgetting his phone in a party. This motivated him to research for solutions. Major issues he found were:

1) About 3.1 million mobile phones are stolen annually

Smartphone Thefts Rise | Locate Stolen or Lost Cell Phone - Consumer Reports News. (n.d.). Smartphone Thefts Rise | Locate Stolen or Lost Cell Phone - Consumer Reports News. Retrieved September 25, 2014, from <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm>

2) 44% of phone thefts are due to owner negligence

Eadicicco, L. (2014, May 7). People Are Willing To Go To Extreme Lengths To Retrieve Their Stolen Smartphones. Business Insider. Retrieved September 25, 2014, from <http://www.businessinsider.com/smartphone-theft-statistics-2014-5>

# THE BIG IDEA: ALERT SYSTEMS

Jon then thought of some solutions:

- Software Apps:
  - Inactivity
  - Distance alarm
  - Heat Tracker
- Supplemental Hardware Designs:
  - Camo-Phone
  - The Sidekick
  - Microchip



# INACTIVITY

To tackle the problem of *forgetting* his phone, he designed this app:

- Time period of inactivity and/or determine if phone is lying horizontal on a flat surface
- If conditions are met, phone beeps or vibrates every 5 minutes so owner is reminded of phone's "presence"



<http://www.jailbreaknation.com/tag/vibrating-time-for-ios>

# DISTANCE TRACKER

To ensure his phone does not ever leave him again, Jon developed an app to:

- Measure distance between him and his phone (with the receiver being a card)
- Set off an alarm if phone ever reaches a distance away (owner forgets phone or thief is pick-pocketing)

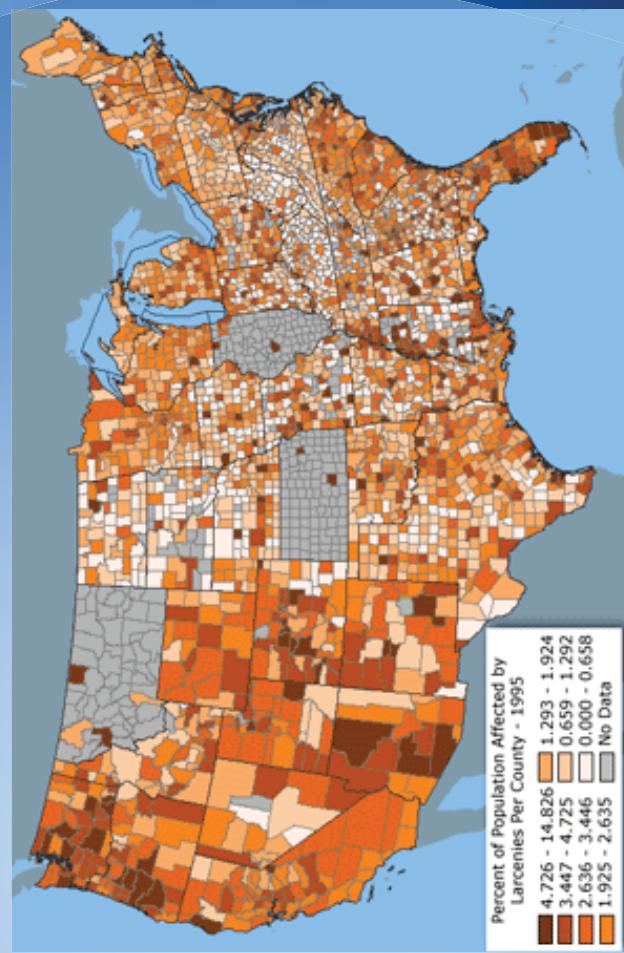


"SYNC Distance Activity Tracker Performance Measurement." Big 5 Sporting Goods.  
N.p., n.d. Web. 30 Sept. 2014.  
<<http://www.big5sportinggoods.com/product/performance-measurement/478242-279305/distance-activity-tracker.html>>

# HEAT TRACKER

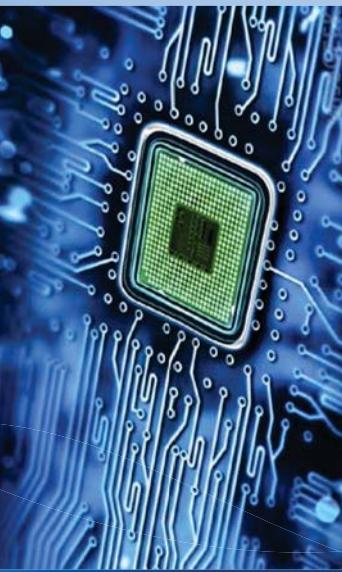
Jon suggested an app that will:

- Determine high-risk, or “heated”, zones where crime is more prevalent
- Notify user when entering such areas



National Atlas, (2014). [image] Available at:  
[http://www.nationalatlas.gov/articles/people/a\\_crime.html](http://www.nationalatlas.gov/articles/people/a_crime.html) [Accessed 28 Sept.. 2014].

# SUPPLEMENTAL HARDWARE DESIGNS



LEFT: Jon's implementation of the *Microchip* supplements the **Distance Tracker app**:

-Chip stays on even if phone is off so owner  
can always track phone's location through  
<http://www.wisegEEK.com/what-are-continuous-inking-systems.htm> card receiver  
RIGHT: Not wanting his phone to be an easy target, Jon came up with the idea of a **Camo-Phone**:



<http://www.dinosaRIA.com/reptiles/>

## ...continued

Jon's use of the sidekick ties in with the Heat Tracker app:

-When alert from Heat Tracker goes off, smartphone users can "detach" a secondary phone and use it temporarily. i.e. losing the sidekick would be a lesser loss



<http://www.trendhunter.com/trends/detachable-phones-patent-filed-for-pda-with-detachable-cellphone>

# ADVANTAGES VS. DISADVANTAGES

Jon compared the gains versus risks and found:

- Apps are simple and easy to install/use: Just download and turn on
- Preventative solutions saves phone and replacement costs
- Easy measures to preventing phone theft
- Cost of such a durable microchip might be too high
- Apps are only functional when phone is on (e.g. phone battery runs out)
- Apps might need to be purchased and paid for use

# Conclusions

- The alert themed solution to phone theft focuses on preventing phone theft
- There are two integrated parts to the alert prevention system:
  - Software applications such as the Distance Tracker and Inactivity apps alert phone user when owner's phone is far from owner. The Heat Tracker helps avoid risk zones
  - Hardware supplements to make the tracker apps applicable



IIT IPRO Team W5B: Nina Townley, Vanessa Arraiz,  
Nicholas Thompson, Maximilian Vitas, Farah Abdul Samad

# Summary

- Our product is a **Phone Theft Prevention System**
- It starts with a recognition software that identifies you through **facial recognition/ fingerprint scanner** when accessing settings (including shortcuts)
- Next it goes through an **emergency mode** where an alarm goes off if it does not recognize the owner/user.
- Then the **tracking device** inside of the phone turns on.
- If the tracker is removed then the device will become **inoperable**

# Assessment of User Needs

- Harder way to access device settings
- Providing a method of tracking the device without the device being connected via wifi, data, gps, etc...
- Harder way to steal a device
- User friendly way of retrieving the device
- Method of maintaining connectivity post theft
- Thieves to have no reason/need to steal a device

# Alternatives

- A more secure means of storage (locking systems and hidden storage)
- Public theft prevention kiosk
- Reward system for users and authority
- Grips for the back of your phone
- Better pockets
- More available statistics for authorities
- Free automatic backup system
- Addressing consumer behavior for avoiding and preventing phone theft by having a instructional card inside the device box with steps of what to do if the device is stolen
- Phone theft department
- Safe mode notification/suggestion when in an unsafe area/situation
- Voice activated alarm/locking system

# Detailed Concept

1. **User Recognition** - When someone tries to access the device settings, the device will ask for facial recognition or fingerprint identification. The device will also ask for facial recognition / fingerprint identification when:
  - a. Turning phone on/off
    - i. Physically turning on/off the phone via the button
    - ii. Options for identification are presented (fingerprint / facial / retinal)
    - iii. ID verification is completed (accepted or rejected)
  - b. In case of invalid entry, after three tries the phone will go into an emergency mode (described in step 2)
    1. Turning airplane mode on/off (no matter where you are located)
    2. This includes alarm, tracking, and notification
  - c. Refer to steps above
2. **Emergency Mode** - Caused by invalid ID verification
  - a. Simultaneous alarm, tracking, and notification occur
    - i. **Alarm**
      1. Very loud noise
      2. Flashing lights - Camera flash goes off
      3. Display - LED screen is disabled due to flashing screen
      4. Vibration
    - ii. **Tracking**
      1. As soon as the tracker has been located within the device, the alarm will turn off and the device will remain disabled
      2. To enable the phone, the user can respond to the notification email with a specific code that they set up when the device is purchased.

# Detailed Concept

- i. **Tracking** - A separate hardware that is installed in the phone when purchased, or can be purchased separately and installed by your provider
  1. When emergency mode is enabled, tracking is activated
  2. If tracking device is removed, step 3 occurs
  3. We will be using a satellite tracking chip
- ii. **Notification**- After the rejection of ID verification, the device will send an email notification to the user and emergency contact
  1. Notification includes last known location (through wifi, data, etc...)
  2. Notification includes a picture of the user attempting to access the device (picture will be taken at each attempt from front and back cameras)
  3. Notification includes information on whether the tracker has been enabled (the alarm is off)
  4. Additional notification will be presented after the device has been reactivated
3. **Self- Destruction**- Complete deactivation/future termination
  - i. Activates a small water pack internal explosion that will completely terminate any further use of the (clearly) stolen device.
  - ii. By eliminating the reason for people to steal a device, the thefts should decrease all by themselves.
  - iii. In a long run, steps 1 ad 2 should be less necessary due to the implementation of step 3.

# Scenarios

- Apply the detailed description above to the following scenarios
  - Public Transportation
  - Public / Crowded Spaces
  - Assault
  - Parties / Events
  - Misplaced Location

# Stakeholder Value Propositions & Business Model

- **Consumers:**
  - keeping devices from being stolen and happiness
- **Carriers:**
  - making profit through tracker activation
  - more customer satisfaction
- **Government:**
  - reduced crime
- **Device Makers:**
  - increased sales of product

# Risks/Mitigations

- **Risks**
  - High impact causing unwanted destruction of device
  - Tracker being too large / expensive
  - Tracker not working due to satellite complications
- **Mitigations**
  - Minimize unwanted destruction by experimenting probabilities on how a hit (phone falling) will not destroy the self-destroying package inside phone.
  - Create a very small, inexpensive tracker for users to purchase

# Implementation Guidance

- **Consumer:**
  - Campaign of our system
    - More safety for the consumer
- **Carrier:**
  - Control over satellite connection (tracker)
  - Another campaign for the interest of the carrier and the benefits of the system.
- **Government:**
  - Once the government endorses our product financially or possibly with certain laws for other parties to cooperate (carriers), they receive 100% benefit, including, less crimes, less theft, national security overall increases and the country looks better.
- **Device Makers:**
  - They receive full responsibility for the production of the tracker and any other hardware necessary. They also get responsibility for the implementation of the new alarm and software that allows the display lock mentioned for the emergency mode. Business, income, and success overall increases. With copyright the idea is provided and with guidance the products are produced and sold through [us] to consumers.

# FCC Cell Phone Theft Challenge Project

III<sup>T</sup> IPRO Team W6A

Neel Patel  
Mateo Garcia  
Randy Remblake  
Lama Almansour  
Corey Gokan

# The Problem

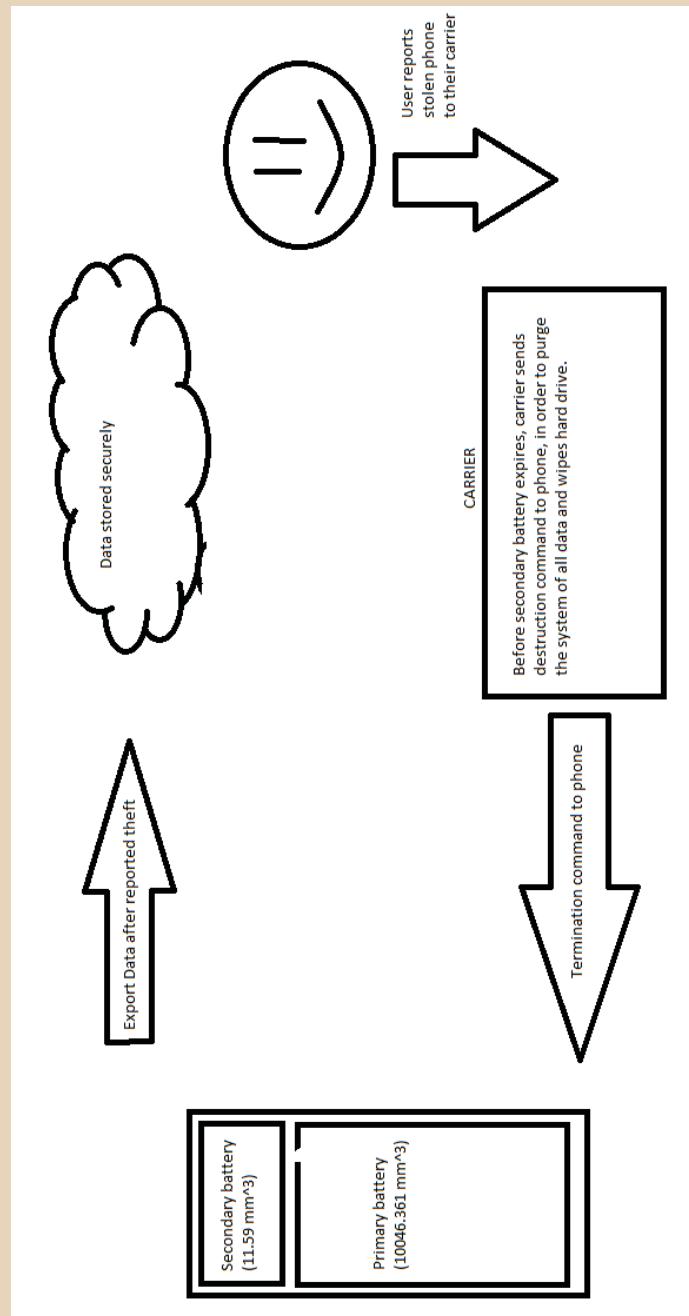
- In cities all over the country cell phone theft is steadily increasing.
- in New York City alone 8,465 apple phones were stolen last year<sup>1</sup>.
- Some are legitimate theft while others are simply misplaced in public places, leaving the user with no real way to retrieve the phone if it isn't where they left it.
- After a theft the phone is quickly turned off by removing the battery or engaging airplane mode, which disconnects the phone from any tracking service which may assist in relocating the phone. Currently the user has little recourse from this action
- Later the phone is sold to aftermarket buyers who can then reuse the phone with little to no repercussions

1. [http://www.huffingtonpost.com/2014/01/15/smartphone-thefts-2013\\_n\\_4598399.html](http://www.huffingtonpost.com/2014/01/15/smartphone-thefts-2013_n_4598399.html)

# Our Solution

- What we are proposing is an effective countermeasure to the phone theft problem
- We have come up with the P.I.D.S.S. system.
  - Preventative
  - Integrated
  - Destructible
  - Security
  - System
- The central idea to this solution is the phone's integrated back-up power supply, which unlike the main power source is non-removable. Engaging airplane mode or removing the main power supply will now require password unlock, adding an extra layer of security to the phone while also granting the ability to keep the phone powered on and trackable. In addition to this there are several other key features which will make the phone overall a vast improvement upon the security of current systems.

# P.I.D.S.S.



# Key Features

- Alternate non-removable power supply to keep GPS engaged and export data
- The phone will be synced to a cloud storage system so that in the result of reported theft, the phone can upload all critical data to it for safe storage.
- All features are integrated into the phone, there is no additional hardware to carry
- Additional security layer in requiring (mandatory)password unlock for main battery removal and engaging airplane mode
- Unauthorized battery removal will result in critical data export followed by full phone hard drive wipe which will render the device essentially useless, with no identity information left behind
- These key features will be heavily marketed in the sales phase, which will serve as a better deterrent to criminals in order to prevent future thefts.

# Scenario

A phone with important data(pictures,homework,etc.) gets stolen which leaves the owner without important and personal information, while the thief gains a mobile phone/camera/media player.

PIDSS addresses the first and major problem, by rendering the phone useless to the thief if he decides to remove the battery/power off the device without authorization. This is usually the case in order to remain anonymous and to eliminate tracking possibilities. Now, the thief cannot resell or reuse the device, which leaves him with a paperweight at best.

Also, the alternate battery exports all personal data on the phone to cloud storage (upon the user reporting the phone stolen), which allows the user to retrieve his/her important information if not previously saved. Additionally, the reserve power source still connects to GPS signal, which can possibly reveal the location of the uninformed thief.

# Value for stakeholders

- **Manufacturer:** The primary cost for this system will fall on the device manufacturer as they would have to design and implement the alternate power supply system. However sales would be increased as there is no direct competitor offering this style of system
- **Consumer:** The consumer would feel a greater level of satisfaction and overall piece of mind knowing that they possess a more secured system. Their worries about identity theft due to phone theft would be greatly reduced.
- **Criminals:** The phone's destructibility features will reduce the ability of the criminal to resell the phone to aftermarket buyers as the phone will only be able to be sold for scrap. In addition the heavy advertising campaign should do well to prevent some of these thefts.

# Business Model

- We need to target a battery producing company to create our second phone battery and have them bear advertising costs to market the phone.
- This will then show the people the need for this security system and in turn the battery, the demand for phones with a second battery will increase due to the advertising.
- We then tell the manufactures about PIDSS and how they can now integrate this system into their phones with the second battery.
- Phones will now by default have PIDSS in them for a security measure against phone theft.

# Risks

- One major risk is the user removing their own main battery without entering the required password, thus wiping their own phone
- A malfunction in the secondary battery could render this system inoperable
- No data connection would prevent critical information from being uploaded to cloud storage, however hard drive wipe would still occur
- Price increase versus additional security

# Implementation

- **Consumer :**  
Campaign for the product:  
1-The information which a trader must give to a consumer before and after making a sale.  
2-How that information should be given.
- **Carrier:**  
Focus on helping to reduce the communication costs, while simplifying the management of the services.
- **Government:**  
1- Do educational programs to teach people to protect themselves from theft.  
2- Improve security in neighbors.

# FCC Challenge

## Smart Device Theft Prevention

### Contents:

Summary	2
Assessment of User Needs	3
Alternatives Considered	4
Concept Description	5
Scenario of Use	6
Stakeholder Value Propositions	7
Business Model	8
Risks/Mitigation	9
Implementation Guidance	10

### IT PRO TEAM W6B

Angel Dimitrov  
Chuka Alintah  
Haoyu Yang  
Roger Ngosso  
Subarno Saha  
Yuanfang Xiang

# Summary

## **Problem Statement:**

The theft of cellular/smart-phones or smart-devices affects the users of the device financially, functionally in terms of being unable to communicate easily, and security-wise in terms of privacy-invasion and theft or loss of data.

## **Solution:**

An indestructible tracking chip running on a separate tiny battery, and a proximity sensor that can be on the user's person at all times.

## **Major functions:** Tracking & Data protection

This solution aims to discourage phone theft by:

- making the device impossible to hide.
- making the device completely useless to unauthorized users.

The solution mitigates the harm on users by:

- destroying all data upon theft
  - making the phone easy to track.
- The dedicated tracking chip that can be either sold to device manufacturers to integrate into phone from the factory or can be sold to be integrated into phone case.

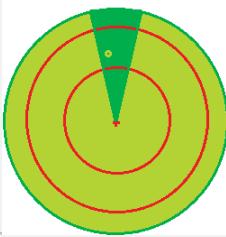
# Assessment of User Needs

- Primary:
  - Regardless of phone's power state or if airplane mode is engaged:
    - phone must **always** be trackable
    - personal data must **always** be safe and be retrievable/deleted after possible theft/loss of phone
    - authorities must be able to be automatically notified if theft occurs
- Secondary:
  - a way to retrieve stolen phone
  - a way to retrieve lost data/contacts
  - a way of finding the phone if it's simply misplaced.

# Alternatives Considered

- **“Phone theft” police**
  - Special police unit to investigate phone theft.
  - Registration of devices to one person so that an unauthorized person cannot access cellular networks and Wi-Fi with the device.
- **Charger paired to device:**
  - Creating a charger (either wireless or conventional wired) that would require being paired and ‘recognized’ by the phone in order to allow charging.
- **Criteria used to pick final concept:**
  - Final concept must be applicable even if phone is turned off or put into airplane mode
  - Concept must accommodate remote control of device into its features

# Concept Description



***The solution is a tracking chip built into the phone with a separate rechargeable battery and a proximity sensing device***

- **Tracking function:**

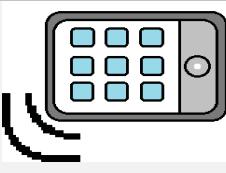
- Irremovable: renders phone useless upon unauthorized tampering.
- Linked only to authorized owner(s)
- Turns on in airplane mode/power off state
- Produce beeps/flash as alarm
- Calls authority automatically
- Alarm sets off when phone is away from proximity device (bracelet)

- **Data Protection:**

- Clone/backup/delete data
- Remotely access

- **Further development:**

- Biometric protection
- Automatic service cancellation
- Lock device
- Call divert
- Password lock at airplane mode
- completely control device



Concept design of proximity bracelet

# Scenario of Use

## (I) Phone misplaced:

User uses bracelet's proximity sensor or beeper/flasher to make the phone ring and follows the noise to the phone (*like find their car in a parking lot.*)

## (II) Phone is pickpocketed:

Bracelet's proximity sensor turns on "theft mode\*", setting off an alarm so that both the user and the people around are informed of the occurrence of theft. The tracker activates and the authority notified. The thief and the phone are easily located.

## (III) User is mugged:

During mugging, "theft mode" is activated when the bracelet is removed in an unauthorized way, setting off the tracker (*the alarm does not turn on as it might put the user in harm's way.*)

## (IV) The thief gets away:

The tracker is active and helps police/carrier locate the thief. All data in the phone is deleted for the sake of data protection. The chip destroys the phone and makes it useless. *This feature is intended to discourage phone theft as well by reducing its resale value to zero.*

\* Theft mode is a set of measures (alarm, beeper, and tracker) which are activated when the user or the proximity sensor can activate when the phone is lost/stolen.

# Stakeholder Value Propositions

- **Consumers**
  - Would be saved the many troubles associated with loss/theft of phone. This would constitute both being spared lost time/productivity as well as lost money as a result of the theft/loss.
- **Police**
  - Police departments would save money as a result of having easy access to the location of phones at all times, if needed.
  - Efforts could be focused on investigating and apprehending more serious crimes
- **Carriers**
  - Potential subscription system for the tracking service could mean extra profit
- **Device manufacturers**
  - Eliminating the black market trade of cell phones would increase manufacturers' end profit.

# Business Model

- **Estimated cost of GPS chip:** ranging from \$19.99 to \$29.00 \*
- **Marketing of the product:**
  - conduct market research to determine prime customer groups and overall interest in the GPS tracker
  - based on data gathered in the market research, an initial promotion in the form of a discount on the price of the tracker will be offered, in order to raise customer's attention and awareness of the product
- **Funding:**
  - gain law enforcement and government's interest in the tracking device, stemming from the decrease in theft occurrence and increase in overall public safety
  - gain government and/or state funding as a result of this support

\* - sources: <http://www.ebay.com/itm/Skylab-UART-Serial-GPS-Module-For-Arduino-uController-with-Breakout-Board-Pins-/271244092864?trksid=p2054897.l5660>  
<http://store.cutedigi.com/mini-gps-receiver-22-channel-with-embedded-antenna/>

# Risks/Mitigations

- **Risk** : Few people are willing to pay extra for the tracking feature
  - **Mitigation** : Include the chip in a carrier's wireless insurance package.
- **Risk** : Tracking chip is hacked
  - **Mitigation** : Investing more into software development to increase security against hacking
- **Risk** : False alarms triggered by the proximity sensors between phone and bracelet
  - **Mitigation** : Alarms can be deactivated by pressing a 'false alarm' button on the bracelet
- **Risk** : Lost/forgotten bracelet causes alarm to trigger
  - **Mitigation**: Enable deactivation of alarm on phone by PIN/password/fingerprint scan.

# Implementation Guidance

- **GPS service**
  - GPS contracts must be established with GPS providers/governments
- **Component integration**
  - Phone manufacturers must accommodate for the space to install the chip within their existing hardware configurations
- **Manufacturing**
  - GPS chip is sourced from outside company and custom platform is built in order to enable to integrate with devices
  - Bracelet with proximity sensor must also be manufactured
- **Installation into product**
  - Phone manufacturers must be given specific instructions on installation within their devices
- **Carrier support**
  - Phone carrier would be in charge of promoting the tracker, ensuring proper functioning of product, serving broken/malfunctioning trackers and replacing broken accompanying bracelets